RESEARCH CENTRE

Bordeaux - Sud-Ouest

IN PARTNERSHIP WITH:

Université de Bordeaux, CNRS

2021

ACTIVITY REPORT

Project-Team LFANT

Lithe and fast algorithmic number theory

IN COLLABORATION WITH: Institut de Mathématiques de Bordeaux (IMB)

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Algorithmics, Computer Algebra and Cryptology

Contents

Project-Team LFANT

Creation of the Project-Team: 2010 January 01

Keywords

Computer sciences and digital sciences

A4.3.1. – Public key cryptography

A8.4. – Computer Algebra

A8.5. – Number theory

A8.10. – Computer arithmetic

Other research topics and application domains

B6. – IT and telecom

B9.5.2. – Mathematics

1 Team members, visitors, external collaborators

Research Scientists

- Andreas Enge [Team leader, Inria, Senior Researcher, HDR]
- Razvan Barbaud [CNRS, Researcher]
- Xavier Caruso [CNRS, Senior Researcher, HDR]
- Fredrik Johansson [Inria, Researcher]
- Aurel Page [Inria, Researcher]
- Alice Pellet-Mary [CNRS, Researcher, from Feb 2021]
- Damien Robert [Inria, Researcher, HDR]
- Benjamin Wesolowski [CNRS, Researcher]

Faculty Members

- Karim Belabas [Univ de Bordeaux, Professor, HDR]
- Guilhem Castagnos [Univ de Bordeaux, Associate Professor, HDR]
- Jean-Paul Cerri [Univ de Bordeaux, Associate Professor]
- Henri Cohen [Univ de Bordeaux, Emeritus]
- Jean-Marc Couveignes [Univ de Bordeaux, Professor, HDR]
- Philippe Elbaz-Vincent [Univ de Montpellier, Professor, from Sep 2021]

PhD Students

- Jared Guissmo Asuncion [Univ de Bordeaux]
- Agathe Beaugrand [Univ de Bordeaux, from Sep 2021]
- Élie Bouscatié [Orange, CIFRE]
- Amaury Durand [Univ de Bordeaux]
- Elie Eid [Univ de Rennes I, until Aug 2021]
- Jean Kieffer [École Normale Supérieure de Paris, until Aug 2021]
- Raphael Pages [Univ de Bordeaux]
- Pavel Solomatin [Université de Leiden - Pays-Bas, until Aug 2021]
- Anne Edgar Wilke [Inria]

Technical Staff

- Bill Allombert [CNRS, Engineer]

Interns and Apprentices

- Abel Laval [Inria, from Mar 2021 until Aug 2021]

Administrative Assistant

- Sabrina Duthil [Inria]

External Collaborator

- Tony Ezome Mintsa [Université des Sciences et Techniques de Masuku - Gabon]

2 Overall objectives

2.1 Presentation

Algorithmic number theory dates back to the dawn of mathematics itself, *cf.* Eratosthenes's sieve to enumerate consecutive prime numbers. With the arrival of computers, previously unsolvable problems have come into reach, which has boosted the development of more or less practical algorithms for essentially all number theoretic problems. The field is now mature enough for a more computer science driven approach, taking into account the theoretical complexities and practical running times of the algorithms.

Concerning the lower level multiprecision arithmetic, folklore has asserted for a long time that asymptotically fast algorithms such as Schönhage–Strassen multiplication are impractical; nowadays, however, they are used routinely. On a higher level, symbolic computation provides numerous asymptotically fast algorithms (such as for the simultaneous evaluation of a polynomial in many arguments or linear algebra on sparse matrices), which have only partially been exploited in computational number theory. Moreover, precise complexity analyses do not always exist, nor do sound studies to choose between different algorithms (an exponential algorithm may be preferable to a polynomial one for a large range of inputs); folklore cannot be trusted in a fast moving area such as computer science.

Another problem is the reliability of the computations; many number theoretic algorithms err with a small probability, depend on unknown constants or rely on a Riemann hypothesis. The correctness of their output can either be ensured by a special design of the algorithm itself (slowing it down) or by an *a posteriori* verification. Ideally, the algorithm outputs a certificate, providing an independent *fast* correctness proof. An example is integer factorisation, where factors are hard to obtain but trivial to check; primality proofs have initiated sophisticated generalisations.

One of the long term goals of the LFANT project team is to make an inventory of the major number theoretic algorithms, with an emphasis on algebraic number theory and arithmetic geometry, and to carry out complexity analyses. So far, most of these algorithms have been designed and tested over number fields of small degree and scale badly. A complexity analysis should naturally lead to improvements by identifying bottlenecks, systematically redesigning and incorporating modern asymptotically fast methods.

Reliability of the developed algorithms is a second long term goal of our project team. Short of proving the Riemann hypothesis, this could be achieved through the design of specialised, slower algorithms not relying on any unproven assumptions. We would prefer, however, to augment the fastest unproven algorithms with the creation of independently verifiable certificates. Ideally, it should not take longer to check the certificate than to generate it.

All theoretical results are complemented by concrete reference implementations in PARI/GP, which allow to determine and tune the thresholds where the asymptotic complexity kicks in and help to evaluate practical performances on problem instances provided by the research community. Another important source for algorithmic problems treated by the LFANT project team is modern cryptology. Indeed, the security of all practically relevant public key cryptosystems relies on the difficulty of some number theoretic problem; on the other hand, implementing the systems and finding secure parameters require efficient algorithmic solutions to number theoretic problems.

3 Research program

3.1 Number fields, class groups and other invariants

Participants: Bill Allombert, Jared Guissmo Asuncion, Karim Belabas, Xavier Caruso, Jean-Paul Cerri, Henri Cohen, Jean-Marc Couveignes, Andreas Enge, Fredrik Johansson, Aurel Page.

Modern number theory has been introduced in the second half of the 19th century by Dedekind, Kummer, Kronecker, Weber and others, motivated by Fermat's conjecture: There is no non-trivial solution in integers to the equation $x^n + y^n = z^n$ for $n \geqslant 3$. Kummer's idea for solving Fermat's problem was to rewrite the equation as $(x+y)(x+\zeta y)(x+\zeta^2 y)\cdots(x+\zeta^{n-1}y) = z^n$ for a primitive n-th root of unity ζ, which seems to imply that each factor on the left hand side is an n-th power, from which a contradiction can be derived.

The solution requires to augment the integers by *algebraic numbers*, that are roots of polynomials in $\mathbb{Z}[X]$. For instance, ζ is a root of $X^n - 1$, $\sqrt[3]{2}$ is a root of $X^3 - 2$ and $\frac{\sqrt{3}}{5}$ is a root of $25X^2 - 3$. A *number field* consists of the rationals to which have been added finitely many algebraic numbers together with their sums, differences, products and quotients. It turns out that actually one generator suffices, and any number field K is isomorphic to $\mathbb{Q}[X]/(f(X))$, where $f(X)$ is the minimal polynomial of the generator. Of special interest are *algebraic integers*, "numbers without denominators", that are roots of a monic polynomial. For instance, ζ and $\sqrt[3]{2}$ are integers, while $\frac{\sqrt{3}}{5}$ is not. The *ring of integers* of K is denoted by $\mathcal{O}_K$; it plays the same role in K as $\mathbb{Z}$ in $\mathbb{Q}$.

Unfortunately, elements in $\mathcal{O}_K$ may factor in different ways, which invalidates Kummer's argumentation. Unique factorisation may be recovered by switching to *ideals*, subsets of $\mathcal{O}_K$ that are closed under addition and under multiplication by elements of $\mathcal{O}_K$. In $\mathbb{Z}$, for instance, any ideal is *principal*, that is, generated by one element, so that ideals and numbers are essentially the same. In particular, the unique factorisation of ideals then implies the unique factorisation of numbers. In general, this is not the case, and the *class group* Cl_K of ideals of $\mathcal{O}_K$ modulo principal ideals and its *class number* $h_K = |\mathrm{Cl}_K|$ measure how far $\mathcal{O}_K$ is from behaving like $\mathbb{Z}$.

Using ideals introduces the additional difficulty of having to deal with *units*, the invertible elements of $\mathcal{O}_K$: Even when $h_K = 1$, a factorisation of ideals does not immediately yield a factorisation of numbers, since ideal generators are only defined up to units. For instance, the ideal factorisation $(6) = (2)\cdot(3)$ corresponds to the two factorisations $6 = 2\cdot 3$ and $6 = (-2)\cdot(-3)$. While in $\mathbb{Z}$, the only units are 1 and -1, the unit structure in general is that of a finitely generated $\mathbb{Z}$-module, whose generators are the *fundamental units*. The *regulator* R_K measures the "size" of the fundamental units as the volume of an associated lattice.

One of the main concerns of algorithmic algebraic number theory is to explicitly compute these invariants (Cl_K and h_K, fundamental units and R_K), as well as to provide the data allowing to efficiently compute with numbers and ideals of $\mathcal{O}_K$; see [51] for a recent account.

The *analytic class number formula* links the invariants h_K and R_K (unfortunately, only their product) to the ζ-function of K, $\zeta_K(s) := \prod_{\mathfrak{p} \text{ prime ideal of } \mathcal{O}_K} (1 - \mathrm{N}\mathfrak{p}^{-s})^{-1}$, which is meaningful when $\Re(s) > 1$, but which may be extended to arbitrary complex $s \neq 1$. Introducing characters on the class group yields a generalisation of ζ- to L-functions. The *generalised Riemann hypothesis (GRH)*, which remains unproved even over the rationals, states that any such L-function does not vanish in the right half-plane $\Re(s) > 1/2$. The validity of the GRH has a dramatic impact on the performance of number theoretic algorithms. For instance, under GRH, the class group admits a system of generators of polynomial size; without GRH, only exponential bounds are known. Consequently, an algorithm to compute Cl_K via generators and relations (currently the only viable practical approach) either has to assume that GRH is true or immediately becomes exponential.

When $h_K = 1$ the number field K may be norm-Euclidean, endowing $\mathcal{O}_K$ with a Euclidean division algorithm. This question leads to the notions of the Euclidean minimum and spectrum of K, and another task in algorithmic number theory is to compute explicitly this minimum and the upper part of this spectrum, yielding for instance generalised Euclidean gcd algorithms.

3.2 Function fields, algebraic curves and cryptology

Participants: Razvan Barbulescu, Karim Belabas, Guilhem Castagnos, Jean-Marc Couveignes, Andreas Enge, Alice Pellet-Mary, Damien Robert, Benjamin Wesolowski, Jean Kieffer.

Algebraic curves over finite fields are used to build the currently most competitive public key cryptosystems. Such a curve is given by a bivariate equation $\mathscr{C}(X,Y)=0$ with coefficients in a finite field $\mathbb{F}_q$. The main classes of curves that are interesting from a cryptographic perspective are *elliptic curves* of equation $\mathscr{C}=Y^2-(X^3+aX+b)$ and *hyperelliptic curves* of equation $\mathscr{C}=Y^2-(X^{2g+1}+\cdots)$ with $g\geqslant 2$.

The cryptosystem is implemented in an associated finite abelian group, the *Jacobian* $\mathrm{Jac}_{\mathscr{C}}$. Using the language of function fields exhibits a close analogy to the number fields discussed in the previous section. Let $\mathbb{F}_q(X)$ (the analogue of $\mathbb{Q}$) be the *rational function field* with subring $\mathbb{F}_q[X]$ (which is principal just as $\mathbb{Z}$). The *function field* of $\mathscr{C}$ is $K_{\mathscr{C}}=\mathbb{F}_q(X)[Y]/(\mathscr{C})$; it contains the *coordinate ring* $\mathscr{O}_{\mathscr{C}}=\mathbb{F}_q[X,Y]/(\mathscr{C})$. Definitions and properties carry over from the number field case $K/\mathbb{Q}$ to the function field extension $K_{\mathscr{C}}/\mathbb{F}_q(X)$. The Jacobian $\mathrm{Jac}_{\mathscr{C}}$ is the divisor class group of $K_{\mathscr{C}}$, which is an extension of (and for the curves used in cryptography usually equals) the ideal class group of $\mathscr{O}_{\mathscr{C}}$.

The size of the Jacobian group, the main security parameter of the cryptosystem, is given by an L-function. The GRH for function fields, which has been proved by Weil, yields the Hasse–Weil bound $(\sqrt{q}-1)^{2g}\leqslant|\mathrm{Jac}_{\mathscr{C}}|\leqslant(\sqrt{q}+1)^{2g}$, or $|\mathrm{Jac}_{\mathscr{C}}|\approx q^g$, where the *genus* g is an invariant of the curve that correlates with the degree of its equation. For instance, the genus of an elliptic curve is 1, that of a hyperelliptic one is $\frac{\deg_X\mathscr{C}-1}{2}$. An important algorithmic question is to compute the exact cardinality of the Jacobian.

The security of the cryptosystem requires more precisely that the *discrete logarithm problem* (DLP) be difficult in the underlying group; that is, given elements D_1 and $D_2=xD_1$ of $\mathrm{Jac}_{\mathscr{C}}$, it must be difficult to determine x. Computing x corresponds in fact to computing $\mathrm{Jac}_{\mathscr{C}}$ explicitly with an isomorphism to an abstract product of finite cyclic groups; in this sense, the DLP amounts to computing the class group in the function field setting.

For any integer n, the *Weil pairing* e_n on $\mathscr{C}$ is a function that takes as input two elements of order n of $\mathrm{Jac}_{\mathscr{C}}$ and maps them into the multiplicative group of a finite field extension $\mathbb{F}_{q^k}$ with $k=k(n)$ depending on n. It is bilinear in both its arguments, which allows to transport the DLP from a curve into a finite field, where it is potentially easier to solve. The *Tate-Lichtenbaum pairing*, that is more difficult to define, but more efficient to implement, has similar properties. From a constructive point of view, the last few years have seen a wealth of cryptosystems with attractive novel properties relying on pairings.

For a random curve, the parameter k usually becomes so big that the result of a pairing cannot even be output any more. One of the major algorithmic problems related to pairings is thus the construction of curves with a given, smallish k.

3.3 Complex multiplication

Participants: Jared Guissmo Asuncion, Karim Belabas, Henri Cohen, Jean-Marc Couveignes, Andreas Enge, Fredrik Johansson, Damien Robert, Anne-Edgar Wilke.

Complex multiplication provides a link between number fields and algebraic curves; for a concise introduction in the elliptic curve case, see Section 1.1 of [56], for more background material, see [55]. In fact, for most curves $\mathscr{C}$ over a finite field, the endomorphism ring of $\mathrm{Jac}_{\mathscr{C}}$, which determines its L-function and thus its cardinality, is an order in a special kind of number field K, called *CM field*. The CM field of an elliptic curve is an imaginary-quadratic field $\mathbb{Q}(\sqrt{D})$ with $D<0$, that of a hyperelliptic curve of genus g is an imaginary-quadratic extension of a totally real number field of degree g. Deuring's lifting theorem ensures that $\mathscr{C}$ is the reduction modulo some prime of a curve with the same endomorphism ring, but defined over the *Hilbert class field* H_K of K.

Algebraically, H_K is defined as the maximal unramified abelian extension of K; the Galois group of H_K/K is then precisely the class group Cl_K. A number field extension H/K is called *Galois* if $H\simeq K[X]/(f)$

and H contains all complex roots of f. For instance, $\mathbb{Q}(\sqrt{2})$ is Galois since it contains not only $\sqrt{2}$, but also the second root $-\sqrt{2}$ of X^2-2, whereas $\mathbb{Q}(\sqrt[3]{2})$ is not Galois, since it does not contain the root $e^{2\pi i/3}\sqrt[3]{2}$ of X^3-2. The *Galois group* $\mathrm{Gal}_{H/K}$ is the group of automorphisms of H that fix K; it permutes the roots of f. Finally, an *abelian* extension is a Galois extension with abelian Galois group.

Analytically, in the elliptic case H_K may be obtained by adjoining to K the *singular value* $j(\tau)$ for a complex valued, so-called *modular* function j in some $\tau \in \mathcal{O}_K$; the correspondence between $\mathrm{Gal}_{H/K}$ and Cl_K allows to obtain the different roots of the minimal polynomial f of $j(\tau)$ and finally f itself. A similar, more involved construction can be used for hyperelliptic curves. This direct application of complex multiplication yields algebraic curves whose L-functions are known beforehand; in particular, it is the only possible way of obtaining ordinary curves for pairing-based cryptosystems.

The same theory can be used to develop algorithms that, given an arbitrary curve over a finite field, compute its L-function.

A generalisation is provided by *ray class fields*; these are still abelian, but allow for some well-controlled ramification. The tools for explicitly constructing such class fields are similar to those used for Hilbert class fields.

4 Application domains

4.1 Number theory

Being able to compute quickly and reliably algebraic invariants is an invaluable aid to mathematicians: It fosters new conjectures, and often shoots down the too optimistic ones. Moreover, a large body of theoretical results in algebraic number theory has an asymptotic nature and only applies for large enough inputs; mechanised computations (preferably producing independently verifiable certificates) are often necessary to finish proofs.

For instance, many Diophantine problems reduce to a set of Thue equations of the form $P(x,y) = a$ for an irreducible, homogeneous $P \in \mathbb{Z}[x,y]$, $a \in \mathbb{Z}$, in unknown integers x, y. In principle, there is an algorithm to solve the latter, provided the class group and units of a rupture field of P are known. Since there is no other way to prove that the full set of solutions is obtained, these algebraic invariants must be computed and certified, preferably without using the GRH.

Deeper invariants such as the Euclidean spectrum are related to more theoretical concerns, e.g., determining new examples of principal, but not norm-Euclidean number fields, but could also yield practical new algorithms: Even if a number field has class number larger than 1 (in particular, it is not norm-Euclidean), knowing the upper part of the spectrum should give a *partial* gcd algorithm, succeeding for almost all pairs of elements of $\mathcal{O}_K$. As a matter of fact, every number field whose unit group has rank strictly greater than 1 is almost norm-Euclidean [53, 52].

Algorithms developed by the team are implemented in the free PARI/GP system for number theory maintained by K. Belabas (see §6.1 for details). They will thus have a high impact on the worldwide number theory community, for which PARI/GP is a reference and the tool of choice.

4.2 Cryptology

Public key cryptology has become a major application domain for algorithmic number theory. This is already true for the ubiquitous RSA system, but even more so for cryptosystems relying on the discrete logarithm problem in algebraic curves over finite fields. For the same level of security, the latter require smaller key lengths than RSA, which results in a gain of bandwidth and (depending on the precise application) processing time. Especially in environments that are constrained with respect to space and computing power such as smrt cards and embedded devices, algebraic curve cryptography has become the technology of choice. Most of the research topics of the LFANT team detailed in §3 concern directly problems relevant for curve-based cryptology: The difficulty of the discrete logarithm problem in algebraic curves (§3.2) determines the security of the corresponding cryptosystems. Complex multiplication, point counting and isogenies (§3.3) provide, on one hand, the tools needed to create secure instances of curves. On the other hand, isogenies have been found to have direct cryptographic applications to hash functions [54] and encryption [57]. Pairings in algebraic curves (§3.2) have proved to be a a rich

source for novel cryptographic primitives. Class groups of number fields (§3.1) also enter the game as candidates for algebraic groups in which cryptosystems can be implemented. However, breaking these systems by computing discrete logarithms has proved to be easier than in algebraic curves; we intend to pursue this cryptanalytic strand of research.

Apart from solving specific problems related to cryptology, number theoretic expertise is vital to provide cryptologic advice to industrial partners in joint projects. It is to be expected that continuing pervasiveness and ubiquity of very low power computing devices will render the need for algebraic curve cryptography more pressing in coming years.

5 Highlights of the year

5.1 Awards

Bill Allombert has been awarded the Médaille de Cristal du CNRS 2020, remise en 2021, for his outstanding work and dedication to the PARI/GP computer algebra system developed in the team. See an article published by the CNRS and a video presenting his work.

Élie Eid has received the ISSAC 2021 Distinguished Student Author Award for his article [22]. Alice Pellet-Mary and Damien Stehlé received the Asiacrypt 2021 best paper award for their article [26].

5.2 Defenses

Damien Robert has defended his habilitation degree with a thesis entitled *Efficient algorithms for abelian varieties and their moduli spaces* [32].

Jean Kieffer has defended his doctoral degree with a thesis entitled *Higher-dimensional modular equations, applications to isogeny computations and point counting* [31].

Élie Eid has defended his doctoral degree with a thesis entitled *On isogeny calculation by solving p-adic differential equations* [30].

6 New software and platforms

6.1 New software

6.1.1 PARI/GP

Keyword: Computational number theory

Functional Description: Pari/Gp is a widely used computer algebra system designed for fast computations in number theory (factorisation, algebraic number theory, elliptic curves, modular forms ...), but it also contains a large number of other useful functions to compute with mathematical entities such as matrices, polynomials, power series, algebraic numbers, etc., and many transcendental functions.

URL: http://pari.math.u-bordeaux.fr/

Contact: Karim Belabas

Participants: Bill Allombert, Karim Belabas, Henri Cohen, Andreas Enge, Aurel Page

Partner: CNRS

6.1.2 Arb

Name: Arb

Keywords: Multiple-Precision, Interval arithmetic, Interval analysis, Computational number theory, Numerical algorithm

Functional Description: C library for arbitrary-precision ball arithmetic

URL: http://arblib.org

Contact: Fredrik Johansson

6.1.3 GNU MPC

Keyword: Arithmetic

Functional Description: Mpc is a C library for the arithmetic of complex numbers with arbitrarily high precision and correct rounding of the result. It is built upon and follows the same principles as Mpfr. The library is written by Andreas Enge, Philippe Théveny and Paul Zimmermann.

Release Contributions: Bug fixes: - Fix an incompatibility problem with GMP 6.0 and before. - Fix an intermediate overflow in asin.

URL: http://www.multiprecision.org/

Contact: Andreas Enge

Participants: Andreas Enge, Mickaël Gastineau, Paul Zimmermann, Philippe Théveny

6.1.4 abelianbnf

Keyword: Computational number theory

Functional Description: abelianbnf is a gp script computing class groups of abelian fields using norm relations in the Galois group. Requires Pari/gp, development version or stable version v2.13+.

URL: https://hal.inria.fr/hal-02961482

Publication: hal-02497890

Contact: Aurel Page

6.1.5 AVIsogenies

Name: Abelian Varieties and Isogenies

Keywords: Computational number theory, Cryptography

Functional Description: AVIsogenies is a Magma package for working with abelian varieties, with a particular emphasis on explicit isogeny computation.

Its prominent feature is the computation of (l,l)-isogenies between Jacobian varieties of genus-two hyperelliptic curves over finite fields of characteristic coprime to l, practical runs have used values of l in the hundreds.

It can also be used to compute endomorphism rings of abelian surfaces, and find complete addition laws on them.

URL: https://www.math.u-bordeaux.fr/~damienrobert/avisogenies/

Contact: Damien Robert

Participants: Damien Robert, Gaëtan Bisson, Romain Cosset

6.1.6 CM

Keyword: Arithmetic

Functional Description: The Cm software implements the construction of ring class fields of imaginary quadratic number fields and of elliptic curves with complex multiplication via floating point approximations. It consists of libraries that can be called from within a C program and of executable command line applications.

Release Contributions: Changes in version 0.3.1 ("Wurstebrei"): - increase minimal version number for mpfrcx to 0.5 and for pari to 2.9. - many internal rewrites - bug fixes

URL: http://www.multiprecision.org/cm/home.html

Contact: Andreas Enge

Participant: Andreas Enge

6.1.7 CMH

Name: Computation of Igusa Class Polynomials

Keywords: Mathematics, Cryptography, Number theory

Functional Description: Cmh computes Igusa class polynomials, parameterising two-dimensional abelian varieties (or, equivalently, Jacobians of hyperelliptic curves of genus 2) with given complex multiplication.

URL: https://www.multiprecision.org/cmh/

Contact: Emmanuel Thomé

Participants: Andreas Enge, Emmanuel Thomé, Regis Dupont

6.1.8 FromLatticesToModularForms

Keyword: Cryptography

Functional Description: FromLatticesToModularForms is a magma package which allows to

- span the isogeny class (of principally polarised abelian varieties) of a power of an elliptic curve by enumerating unimodular hermitian lattices - compute the abelian variety A corresponding to a given lattice by exhibiting a kernel and an isogeny from Eĝ to A - A is represented by its theta null point (of level 2 or 4) in such a way that we give an affine lift of the theta null point corresponding to the pushforward of the standard diagonal differential dx/y on Eĝ - in particular one can evaluate rational modular forms on A - in dimension 2 or 3 we also provide code to recognize when A is a Jacobian and if so to find the corresponding curve.

URL: https://gitlab.inria.fr/roberdam/fromlatticestomodularforms

Contact: Damien Robert

6.1.9 KleinianGroups

Keywords: Computational geometry, Computational number theory

Functional Description: KleinianGroups is a Magma package that computes fundamental domains of arithmetic Kleinian groups.

URL: http://www.normalesup.org/~page/Recherche/Logiciels/logiciels-en.html

Publication: hal-00703043

Contact: Aurel Page

6.1.10 MPFRCX

Keyword: Arithmetic

Functional Description: Mpfrcx is a library for the arithmetic of univariate polynomials over arbitrary precision real (Mpfr) or complex (Mpc) numbers, without control on the rounding. For the time being, only the few functions needed to implement the floating point approach to complex multiplication are implemented. On the other hand, these comprise asymptotically fast multiplication routines such as Toom-Cook and the FFT.

Release Contributions: Changes in version 0.6: - new functions mpfrx_eval and mpcx_eval for evaluating polynomials in a single argument using a Horner scheme, this complements the existing functions mpcx_multieval and mpfrx_multieval - new convenience functions * mpcx_mul_c, mpcx_mul_fr, mpcx_mul_si, mpcx_mul_ui, mpfrx_mul_fr, mpfrx_mul_si, mpfrx_mul_ui for multiplying polynomials by constants of various types * mpcx_mul_x, mpfrx_mul_x for multiplying by powers of the variable - bug: make multieval work for polynomials of degree <= 1

URL: http://www.multiprecision.org/mpfrcx/home.html

Contact: Andreas Enge

Participant: Andreas Enge

6.1.11 PariTwine

Name: PariTwine

Keywords: Arithmetic, Symbolic computation, Number theory

Functional Description: PariTwine is a glue library between the system for computer algebra and number theory PARI/GP and a number of other mathematics libraries, currently GMP, GNU MPFR, GNU MPC, FLINT, ARB and CMH.

URL: https://www.multiprecision.org/paritwine/

Contact: Andreas Enge

Participants: Andreas Enge, Fredrik Johansson

6.1.12 SageMath

Name: SageMath

Keywords: Graph algorithmics, Graph, Combinatorics, Probability, Matroids, Geometry, Numerical optimization

Scientific Description: SageMath is a free open-source mathematics software system. It builds on top of many existing open-source packages: NumPy, SciPy, matplotlib, Sympy, Maxima, GAP, FLINT, R and many more. Access their combined power through a common, Python-based language or directly via interfaces or wrappers.

Functional Description: SageMath is a free mathematics software system written in Python and combining a large number of mathematical libraries under a common interface.

INRIA teams contribute in different ways to the software collection. COATI adds new graph algorithms along with their documentations and the improvement of underlying data structures. LFANT contributes through libraries such as ARB and PARI/GP, and directly through SageMath code for algebras and ring and field extensions.

Release Contributions: See http://www.sagemath.org/changelogs/

URL: http://www.sagemath.org/

Contact: David Coudert

Participants: David Coudert, Xavier Caruso

6.1.13 Euclid

Keyword: Number theory

Functional Description: Euclid is a program to compute the Euclidean minimum of a number field. It is a stand-alone program depending on the PARI library.

URL: http://www.math.u-bordeaux1.fr/~plezowsk/euclid/index.php

Contact: Jean-Paul Cerri

Participants: Jean-Paul Cerri, Pierre Lezowski

6.1.14 CUBIC

Keyword: Number theory

Functional Description: Cubic is a stand-alone program that prints out generating equations for cubic fields of either signature and bounded discriminant. It depends on the Pari library. The algorithm has quasi-linear time complexity in the size of the output.

URL: http://www.math.u-bordeaux.fr/~belabas/research/software/cubic-1.2.tgz

Contact: Karim Belabas

Participant: Karim Belabas

6.1.15 APIP

Name: Another Pairing Implementation in PARI

Keywords: Cryptography, Computational number theory

Scientific Description: Apip , Another Pairing Implementation in PARI, is a library for computing standard and optimised variants of most cryptographic pairings.

The following pairings are available: Weil, Tate, ate and twisted ate, optimised versions (à la Vercauteren–Hess) of ate and twisted ate for selected curve families.

The following methods to compute the Miller part are implemented: standard Miller double-and-add method, standard Miller using a non-adjacent form, Boxall et al. version, Boxall et al. version using a non-adjacent form.

The final exponentiation part can be computed using one of the following variants: naive exponentiation, interleaved method, Avanzi–Mihailescu's method, Kato et al.'s method, Scott et al.'s method.

Part of the library has been included into Pari/Gp proper.

Functional Description: APIP is a library for computing standard and optimised variants of most cryptographic pairings.

URL: http://www.lix.polytechnique.fr/~milanj/apip/apip.xhtml

Contact: Andreas Enge

Participant: Jérôme Milan

6.1.16 Nemo

Name: Nemo

Keywords: Computer algebra system (CAS), Symbolic computation

Functional Description: A computer algebra package for the Julia programming language

URL: http://nemocas.org

Contact: Fredrik Johansson

Partner: Technische Universität Kaiserslautern (UniKL), Allemagne

6.2 New platforms

6.2.1 Relaxed p-adic numbers

Participants: Xavier Caruso.

X. Caruso wrote a SageMath package implementing relaxed p-adic numbers as introduced a few years ago by van der Hoeven et al. This implementation is part of the standard distribution of SageMath since version 9.4.

6.2.2 From Lattices To Modular Forms

Participants: Damien Robert.

Code implementing the article [17] for spanning the isogeny class of products of elliptic curves and computing modular forms (and related obstruction) on them is available as a MAGMA package called FromLatticesToModularForm.

7 New results

7.1 Coding theory and cryptology

Participants: Razvan Barbulescu, Guilhem Castagnos, Aurel Page, Alice Pellet-Mary, Benjamin Wesolowski.

Classical public-key cryptography. The presumed hardness of the discrete logarithm problem (DLP) in finite fields (or other families of groups) is a foundation of classical public-key cryptography. It has recently been discovered that the DLP is much easier than previously believed in an important family: finite fields of *small characteristic*. Algorithms of quasi-polynomial complexity have been discovered.

Pomerance proved in 1987 that the DLP in finite fields of fixed characteristic can be solved in subexponential time. All improvements from that point to the discrovery of the first quasi-polynomial algorithms have been heuristic. In [18], T. Kleinjung and B. Wesolowski prove that this problem can indeed be solved in quasi-polynomial expected time, bridging the gap between the best heuristic and rigorous algorithms. More generally, they prove that it can be solved in the field of cardinality p^n in expected time $(pn)^{2\log_2(n)+O(1)}$.

In [16], R. Granger, T. Kleinjung, A. K. Lenstra, B. Wesolowski and J. Zumbrägel demonstrate the practicality of these new methods through the computation of a discrete logarithm in $\mathbb{F}_{2^{30750}}$, breaking by a large margin the previous record, which was set in January 2014 by a computation in $\mathbb{F}_{2^{9234}}$.

Many interesting applications of pattern matching like deep packet inspection target very sensitive data. In particular, spotting illegal behaviour in internet traffic conflicts with legitimate privacy requirements. The compromise between traffic analysis and privacy can be achieved through searchable encryption. However, as the traffic data is a stream and as the patterns to search are bound to evolve over time (e.g. new virus signatures), these applications require a kind of searchable encryption that provides more flexibility than the classical schemes. We indeed need to be able to search for patterns of variable sizes in an arbitrary long stream that has potentially been encrypted prior to pattern identification.

In [20], É. Bouscatié, G. Castagnos and O. Sanders propose new public key encryption schemes that allows flexible pattern matching. Using pairings of elliptic curves, they propose two constructions. The first one dramatically reduces the size of the public key compared to previous solutions but its security is based on a strong algorithmic assumption. The second construction manages to retain most of the good features of the first one while exclusively relying on a simple assumption, a (static) variant of the decisional Diffie-Hellman assumption, which solves the security problem of previous works.

Timed commitments are the timed analogue of standard commitments, where the commitment can be non-interactively opened after a pre-specified amount of time passes. Timed commitments have a large spectrum of applications, such as sealed bid auctions, fair contract signing, fair multi-party computation, and cryptocurrency payments. Unfortunately, all practical constructions rely on a (private-coin) trusted setup and do not scale well with the number of participants.

In [27], S. Thyagarajan, G. Castagnos, F. Laguillaumie and G. Malavolta set out to resolve these two issues and propose an efficient timed commitment scheme that also satisfies the strong notion of CCA-security. Specifically, the scheme has a transparent (i.e. public-coin) one-time setup and the amount of sequential computation is essentially independent of the number of participants. As a key technical ingredient, they propose the first (linearly) homomorphic time-lock puzzle with a transparent setup, from class groups of imaginary quadratic order.

To demonstrate the applicability of their scheme, they use it to construct a new distributed randomness generation protocol, where n parties jointly sample a random string. This protocol is the first to simultaneously achieve high scalability in the number of participants, transparent one-time setup, lightning speed in the optimistic case where all parties are honest, and ensures that the output random string is unpredictable and unbiased, even when the adversary corrupts $n-1$ parties.

The note [50] was written by B. Wesolowski in 2016, but never published before. Some of the ideas it contains led to the construction of the first efficient verifiable delay function by the same author. Other ideas, such as *fading signatures* and a discussion on their (in-)feasibility, never appeared in public work.

The elliptic curve method of factorisation (ECM) is a building block of the best algorithms for factoring and computing discrete logarithms. ECM has a rigorous proof of complexity under the celebrated conjecture of existence of smooth numbers in short intervals. However, it does not correspond to the variant which is implemented and studied in the literature of ECM-friendly curves. In [35] R. Barbulescu proves that the celebrated conjecture of Elliott-Halberstam implies this latter variant in the case of CM elliptic curves, for a smoothness bound larger than the one used in ECM. Then he proves that a recent conjecture of Pollack implies the correctness in the general case.

Many quantum algorithms have been developed with time-complexity in mind but the evolution of the technology made it important to create space-time tradeoffs where the space is the number of qbits. In a technical report [34], R. Barbulescu studies the case in which one can factors numbers up to 100 bits on a quantum computer in negligible time. A precise analysis of the algorithm and the difficult parameter tuning leads to the conclusion that one could obtain factoring records using classical-quantum algorithms, but this has a negligible implication on the security of the RSA cryptosystem.

Post-quantum cryptography. It has been known since the work of Shor in 1994 that a functional, large-scale quantum computer would be able to break most classical public-key cryptosystems deployed today. The cryptographic community has since then investigated new families of *post-quantum* cryptosystems, meant to resist the advance of quantum computing. *Lattice-based cryptography*, one of the leading

post-quantum candidates, relies on the presumed hardness of certain computational problems in euclidean lattices. There is strong confidence in the hardness of these problems in general, but the use of algebraic lattices (necessary for efficiency or advanced functionalities) opens new angles of attack. In [14], R. Cramer, L. Ducas and B. Wesolowski expose an unexpected quantum hardness gap between generic lattices and an important family of algebraic lattices, so-called *cyclotomic ideal lattices*. This journal article expands upon preliminary results presented at Eurocrypt 2017. In [26], A. Pellet-Mary and D. Stehlé prove some security guarantees for the algorithmic problem NTRU, used in many post-quantum cryptographic primitives.

Coding theory. In [19], C. Maire and A. Page revisit a construction due to Lenstra and Guruswami by generalising it to unit groups of division algebras. Lenstra and Guruswami described number field analogues of the algebraic geometry codes of Goppa. Recently, Maire and Oggier generalised these constructions to other arithmetic groups: unit groups in number fields and orders in division algebras; they suggested to use unit groups in quaternion algebras, but could not completely analyse the resulting codes. Maire and Page prove that the noncommutative unit group construction yields asymptotically good families of codes for the sum-rank metric from division algebras of any degree, and estimate the smallest possible size of the alphabet in terms of the degree of the algebra.

In [12], X. Caruso develops a theory of residues for skew rational functions, that are elements of the ring of fractions of a skew polynomial field $K[X;\theta]$ (where θ is a ring endomorphism of K). He notably establishes a formula for changing variables and proves a skew analogue of the theorem of residues.

In [39], X. Caruso et A. Durand use (and extend) the theory of residues of Ore rational functions introduced in the aforementioned paper [12] in order to give a description of the duals of linearized Reed-Solomon codes. Their construction shows in particular that, under some assumptions on the base field, the class of linearized Reed-Solomon codes is stable under duality.

7.2 Number fields and symbolic computation

Participants: Aurel Page, Jean Kieffer, Raphaël Pagès.

In [25], R. Pagès designs an algorithm for computing the p-curvatures of a differential operator with rational coefficients for p varying in the set of prime numbers until a given upper bound N. His algorithm exhibits a quasi-linear complexity with respect to N, which correspond to an average polynomial time in $\log p$.

Given an integer polynomial P of degree D with coefficients of height H, evaluating P at small integers will give values of height $\tilde{O}(H)$. However reconstructing P from $D+1$ evaluation points of small height h will only give a bound of $\tilde{O}(Dh)$ for the height of the coefficients of P. In [48] Kieffer explains how, when given more evaluated points of small height, one can recover a bound of (roughly) $\tilde{O}(h)$. This result is extended to a rational function Q over a number field.

A. Page and his coauthors have updated their preprint [36], in which they analyse in detail the subfield method to accelerate the computation of S-units and class groups in the Galois case. They introduce a new group-theoretic notion of norm relation that extends classical ones and give criteria for the existence of such relations. They provide subfield-based algorithms for the computation of invariants of number fields in the presence of a norm relation and prove a polynomial-time reduction to the subfields. They compute class groups of number fields of large degree that go far beyond previous records, both under GRH (degree 1728) and unconditionally (degree 576).

7.3 Modular forms and L-functions

Participants: Razvan Barbulescu, Karim Belabas, Henri Cohen, Fredrik Johansson, Damien Robert.

K. Belabas and H. Cohen have published a book on numerical algorithms for number theory[29], together with extensive PARI/GP programs available from the authors' website. The goal of the book is to present a number of analytic and arithmetic numerical methods used in number theory, with a particular emphasis on the ones which are less known than they should be, although very classical tools are also mentioned. Note that, as is very often the case in number theory, numerical methods are wanted to give sometimes hundreds if not thousands of decimal places of accuracy.

The best algorithms for integer factorisation use a non-negligible proportion of the time to enumerate smaller integers and to test if all their prime factors are below a given bound. A lot of effort has been spent in the literature to improve the best algorithm for this task, the elliptic curve method (ECM). In [11], R. Barbulescu and his doctoral student S. Shinde give a simple method which allows to find rapidly, in a unified manner, all the previously known families of elliptic curves for ECM. They prove that there are precisely 1525 ECM-friendly families using the theory of modular forms.

In [17], M. Kirschmer, F. Narbonne, C. Ritzenthaler and D. Robert give an algorithm to span the isomorphism classes of principally polarised abelian varieties in the isogeny class of E^g, where E is an elliptic curve. The varieties are first described as hermitian lattices over (not necessarily maximal) quadratic orders and then geometrically in terms of their algebraic theta null point. They also show how to algebraically compute Siegel modular forms of even weight given as polynomials in the theta constants by a careful choice of an affine lift of the theta null point. They then use these results to give an algebraic computation of Serre's obstruction for principally polarized abelian threefolds isogenous to E^3 and of the Igusa modular form in dimension 4. They illustrate these algorithms with examples of curves with many rational points over finite fields.

H. Cohen surveys a number of different methods for computing $L(\chi, 1-k)$ for a Dirichlet character χ, with particular emphasis on quadratic characters, in [41]. The main conclusion is that when k is not too large (for instance $k \leqslant 100$) the best method comes from the use of Eisenstein series of half-integral weight, while when k is large the best method is the use of the complete functional equation, unless the conductor of χ is really large, in which case the previous method again prevails.

In [46], F. Johansson shows that the Dirichlet L-function values $L(s)$ can be approximated numerically in subquadratic time with respect to the bit precision, for suitably bounded algebraic numbers s. This improves on previous algorithms with quadratic complexity and leads to improved complexity bounds for computing a variety of mathematical constants as well as certain combinatorial sequences such as Euler numbers.

7.4 Complex multiplication and isogenies of abelian varieties

Participants: Jared Asuncion, Xavier Caruso, Jean-Marc Couveignes, Elie Eid, Tony Ezome, Jean Kieffer, Abdoulaye Maiga, Damien Robert, Benjamin Wesolowski.

In [44], E. Eid designs an algorithm for computing explicit rational representations of $(\ell,\dots,\ell)$-isogenies between Jacobians of hyperelliptic curves of arbitrary genus over a p-adic field K. His algorithm has a quasi-linear complexity in ℓ as well as in the genus of the curve. As an application, he obtains a new efficient algorithm for the computation of the ℓ-division polynomials over the Jacobian of a hyperelliptic curve.

J. Asuncion shows in [33] how class fields of quartic CM fields can be obtained explicitly using CM constructions of higher moduli. He gives an explicit upper bound on the modulus and an algorithm for finding the smallest modulus, and he provides examples of previously unreachable class fields.

In [43], J.-M. Couveignes and T. Ezome study the complexity of multiplication in the context of normal bases of finite field extensions. They define the equivariant complexity of such an extension and prove general and specific bounds for it using the geometry of covers of curves and isogenies of Jacobian varieties.

A. Maiga and D. Robert examine in [24] modular polynomials for abelian surfaces with good reduction modulo 2, which enables them to compute canonical lifts of such surfaces over a finite field of characteristic 2 and to ultimately deduce their cardinality, the main security parameter for hyperelliptic curve

cryptosystems. These modular polynomials use absolute invariants with good reduction modulo 2. They also explain how to lift the curve.

In [47], J. Kieffer gives degree and height bounds for modular equations on PEL Shimura varieties in terms of their level. In particular, his result answers previous questions about Hilbert and Siegel modular polynomials and the complexity of algorithms manipulating them.

In [13], X. Caruso, É. Eid and Reynald Lercier design a new algorithm for computing isogenies between elliptic curves over an extension of the field of 2-adic numbers. Their methods rely on a highly efficient and numerically stable algorithm for solving certain types of nonlinear singular 2-adic differential equations. From this work, they deduce fast algorithms for computing isogenies between elliptic curves in characteristic 2 and generating irreducible polynomials of large degrees over $\mathbb{F}_2$.

In [22], É. Eid extends the above strategy to the case of isogenies between Jacobians of hyperelliptic curves in odd characteristic. The obtained algorithm has quasi-linear complexity with respect to the degree of the isogeny.

In [28], B. Wesolowski proves that the path-finding problem in ℓ-isogeny graphs and the problem of computing the endomorphism ring of supersingular elliptic curves are equivalent under reductions of polynomial expected time, assuming the generalised Riemann hypothesis. The presumed hardness of these problems is foundational for isogeny-based cryptography.

In [49], D. Lubicz and D. Robert explain how to recover the full matrix of the Frobenius action when computing canonical lifts of abelian varieties. Canonical lifts were introduced by Satoh to count the number of points of an elliptic curve over a finite field of small characteristic. The extension of this algorithm to abelian varieties computes the action of the Frobenius via modular forms, hence only recovers its determinant action. This is not always enough to obtain the full characteristic polynomial (hence the number of points) in higher dimension, and even when possible require an expansive LLL computation. In this article, the authors explain how to use isogenies and tangent spaces to recover the full matrix directly. Furthermore they explain how to work this out on the Kummer variety, which is more practical from the algorithmic view point, but not smooth at the neutral point. The resulting algorithm is of independent interest.

7.5 Geometry and arithmetic over the p-adics

Participants: Xavier Caruso.

In [21], continuing their work on the computation of Gröbner bases over Tate algebras, X. Caruso, T. Vaccon and T. Verron give an adaptation of the FGLM algorithm in this context. Beyond making possible a fast change of ordering, their algorithm can also be used to change the radii of convergence, making then effective the bridge between algebraic geometry over the p-adics and rigid geometry.

In [38], X. Caruso, A. David and A. Mézard study the relationships between certain Galois deformation spaces and the corresponding Kisin varieties (endowed with additional structures). They prove notably that the latter determines the number of irreducible components of the former and give fast algorithms to enumerate them.

In [37], X. Caruso studies the distribution of the roots of a random p-adic polynomial in an algebraic closure of $\mathbb{Q}_p$. He proves that the mean number of roots generating a fixed p-adic field K depends mostly on the discriminant of K, an extension containing less roots when it gets more ramified. He proves further that, for any positive integer r, a random p-adic polynomial of sufficiently large degree has about r roots on average in extensions of degree at most r. Beyond the mean, he also studies higher moments and correlations between the number of roots in two given subsets of $\mathbb{Q}_p$. In this perspective, he notably establishes results highlighting that the roots tend to repel each other and he quantifies this phenomenon.

7.6 Complex and p-adic multiprecision arithmetic

Participants: Xavier Caruso, Fredrik Johansson.

In [23], F. Johansson describes Calcium, a new library for exact real and complex arithmetic with the ability to prove equalities for a large class of numbers.

In [15], E. Friedman, F. Johansson and G. Ramirez-Raposo prove a conjecture from 2014 by Katok, Katok and Rodriguez Hertz, rigorously establishing the minimal value of the Fried average entropy for higher-rank Cartan actions.

In [45] F. Johansson provides an extensive review of multiprecision algorithms for computing the gamma function and makes some improvements to the fastest known algorithms.

In [40], X. Caruso, M. Mezzarobba, N. Takayama and T. Vaccon give algorithms for computing values of many p-adic elementary and special functions, including logarithms, exponentials, polylogarithms, and hypergeometric functions. All their algorithms feature a quasi-linear complexity with respect to the target precision and most of them are based on an adaptation to the p-adic setting of the binary splitting and bit-burst strategies.

8 Bilateral contracts and grants with industry

8.1 Bilateral contracts with industry

Participants: Guilhem Castagnos.

G. Castagnos has a three years contract with Orange (Orange Labs Cesson-Sévigné) for the supervision of the PhD of Élie Bouscatié (Thèse CIFRE) from November 2020 to November 2023.

9 Partnerships and cooperations

9.1 International initiatives

9.1.1 Participation in other International Programs

ANR-NSF CHARM – Cryptographic Hardness of Module Lattices

Participants: Bill Allombert, Karim Belabas, Aurel Page, Alice Pellet-Mary, Benjamin Wesolowski.

Project URL

Duration: 2021–2024

One of the most promising candidates for quantum-resistant cryptography is lattice-based cryptography. In this framework, the security is inherited from the presumed computational intractability of certain problems on high-dimensional Euclidean lattices. Efficiency and functionality of lattice-based cryptography can be significantly improved by switching the underlying hardness assumptions to module lattices, which possess additional algebraic structure. For this reason, hardness assumptions for problems on algebraically-structured lattices have received significant attention in recent studies.

This ANR-NSF project aims at clarifying the landscape of module lattice problems. The prime objective is to provide a clearer understanding of the intractability of module lattice problems, via improved reductions between them and improved dedicated algorithms.

CNRS-DERCI Soutien aux collaborations avec l'Afrique subsahrienne

Participants: Jean-Marc Couveignes, Cécile Armana, Christian Maire, Tony Ezome.

Duration: 2021–2022

This project called REDGATE (recherche et encadrement doctoral en géométrie algébrique et théorie des nombres effectives en Afrique) aims at supporting the activities of the Pole of Research in Mathematics and Applications in Africa , a network of 60 African mathematicians, in the fields of algebraic geometry, number theory and their applications to information theory. The two main activities supported by the REDGATE project are research schools for graduate and PhD students in Africa and scientific visits to enhance collaborations.

9.2 International research visitors

9.2.1 Visits of international scientists

Other international visits to the team

Koen de Boer

Status: PhD student

Institution of origin: CWI, Amsterdam

Country: the Netherlands

Dates: from 01/11/2021 to 20/11/2021

Context of the visit: research collaboration with A. Page, A. Pellet-Mary and B. Wesolowski

Mobility program/type of mobility: research stay

9.3 National initiatives

9.3.1 ANR ALAMBIC – AppLicAtions of MalleaBIlity in Cryptography

Participants: Guilhem Castagnos.

Project URL

Duration: 2016 – 2022

The ALAMBIC project was planned to end in October 2020, but was prolonged due to the pandemics to April 2021 and then to April 2022.

The ALAMBIC project is a research project formed by members of the INRIA Project-Team CASCADE of ENS Paris, members of the AriC INRIA project-team of ENS Lyon, and members of the CRYPTIS of the university of Limoges. G. Castagnos is an external member of the team of Lyon for this project.

Non-malleability is a security notion for public key cryptographic encryption schemes that ensures that it is infeasible for an adversary to modify ciphertexts into other ciphertexts of messages which are related to the decryption of the first ones. On the other hand, it has been realised that, in specific settings, malleability in cryptographic protocols can actually be a very useful feature. For example, the notion of homomorphic encryption enables specific types of computations to be carried out on ciphertexts and to generate an encrypted result which, when decrypted, matches the result of operations performed on the plaintexts. The homomorphic property can be used to create secure voting systems, collision-resistant hash functions, private information retrieval schemes, and fully homomorphic encryption enables widespread use of cloud computing by ensuring the confidentiality of processed data.

The aim of the ALAMBIC project is to investigate further theoretical and practical applications of malleability in cryptography. More precisely, this project focuses on three different aspects: secure computation outsourcing and server-aided cryptography, homomorphic encryption and applications and “paradoxical” applications of malleability.

9.3.2 ANR FLAIR – Familles de fonctions L: analyse, interactions, résultats effectifs

Participants: Bill Allombert, Karim Belabas, Jean-Marc Couveignes.

ANR URL
Project URL
Duration: 2017–2021

Building on the unifying theme of L-functions, the FLAIR project synthetises complementary point of views from multiple domains: analytic approaches for classical L-functions, the theory of Artin L-functions through the Langlands program, geometric L-functions in the spirit of the Weil conjectures and the Grothendieck school, p-adic L-functions.

Developping systematically the emerging notion of good families of L-functions, the project members study concrete problems of an arithmetic, analytic or geometric nature, with constant interaction between theoretical and numerical considerations, algorithms and implementations.

9.3.3 ANR CLAP-CLAP – The p-adic Langlands correspondence: a constructive and algorithmical approach

Participants: Xavier Caruso, Jean-Marc Couveignes.

ANR URL
Duration: 2018–2022

The p-adic Langlands correspondence has become nowadays one of the deepest and the most stimulating research programmes in number theory. It was initiated in France in the early 2000's by Breuil and aims at understanding the relationship between the p-adic representations of p-adic absolute Galois groups on the one hand and the p-adic representations of p-adic reductive groups on the other hand. Beyond the case of $\mathrm{GL}_2(\mathbb{Q}_p)$, which is now well established, the p-adic Langlands correspondence remains quite obscure, and mysterious new phenomena enter the scene; for instance, on the $\mathrm{GL}_n(F)$-side one encounters a vast zoology of representations which seems extremely difficult to organise.

The CLAP-CLAP ANR project aims at accelerating the expansion of the p-adic Langlands program beyond the well-established case of $\mathrm{GL}_2(\mathbb{Q}_p)$. Its main originality consists in its very constructive approach mostly based on algorithmics and calculations with computers at all stages of the research process. We pursue three different objectives closely related to our general aim:

1. draw a conjectural picture of the (still hypothetical) p-adic Langlands correspondence in the case of GL_n,

2. compute many deformation spaces of Galois representations and make the bridge with deformation spaces of representations of reductive groups,

3. design new algorithms for computations with Hilbert and Siegel modular forms and their associated Galois representations.

This project is also the opportunity to contribute to the development of the mathematical software SAGEMATH and to the expansion of computational methodologies.

9.3.4 ANR CIAO – Cryptography, Isogenies and Abelian varieties Overwhelming

Participants: Jean-Marc Couveignes, Jean Kieffer, Aurel Page, Damien Robert.

ANR URL
Duration: 2019–2023

The CIAO ANR project is a young researcher ANR project led by Damien Robert.

The aim of the CIAO project is to study the security and to improve the efficiency of the SIDH (supersingular isogenies Diffie Helmann) protocol, which is one of the post-quantum cryptographic project submitted to NIST, where it passed the first round of selections.

The project includes all aspects of SIDH, from theoretical ones (computing the endomorphism ring of supersingular elliptic curves, generalisation of SIDH to abelian surfaces) to more practical aspects like arithmetic efficiency and fast implementations, and also extending SIDH to more protocols than just key exchange.

Applications of this project are to improve the security of communication in a context where the currently used cryptosystems are vulnerable to quantum computers. Beyond post-quantum cryptography, isogeny based cryptosystems also allow one to construct new interesting cryptographic tools, such as verifiable delay functions used in block chains.

9.3.5 ANR NUSCAP – Sûreté numérique pour les preuves assistées par ordinateur

Participants: Fredrik Johansson.

ANR URL
Duration: 2021–2025

The NuSCAP project aims at developing theorems, algorithms and software to improve the numerical safety of computer-aided proofs in mathematics.

9.3.6 ANR MELODIA – Méthodes pour les variétés abéliennes de petite dimension

Participants: Benjamin Wesolowski.

ANR URL
Duration: 2021–2025

The MELODIA ANR project is a young researcher ANR project led by Gaetan Bisson.

Its main objective is to systematically study the algebraic structure of isogeny graphs of abelian varieties, with a view to attacking important open problems in number theory and cryptography.

It focuses on low-dimensional abelian varieties defined over finite fields and tackles the following (closely related) problems: describing the abstract structure of the isogeny graph; computing the endomorphism ring of an abelian variety; constructing an abelian variety with a prescribed number of points; obtaining a Gross-Zagier formula for such varieties.

The case of supersingular elliptic curves is of particular interest as the presumed hardness of the corresponding computational problems is of foundational importance to isogeny-based cryptography. The MELODIA project aims at pinpointing the precise hardness of these problems, to guide the choice of secure cryptographic parameters for a variety of post-quantum protocols.

9.3.7 ANR SANGRIA – Secure distributed computAtioN - cryptoGRaphy, combinatorIcs and computer Algebra

Participants: Guilhem Castagnos, Alice Pellet-Mary, Benjamin Wesolowski.

Project URL
Duration: 2021–2025

Secure distributed computation has long stood in the realm of theoretical cryptography, but it was known to have the potential of providing a disruptive change for practical security solutions. The concept was introduced by Yao in the 1980s and it allows mutually distrusting parties to run joint computations without disclosing any participant's private inputs. New cryptographic tools have been invented in recent years (e.g. fully-homomorphic encryption, functional encryption, succinct proof systems, and so on). These constructions have opened the door to applications that were previously believed unattainable in practice (e.g. Cloud Computing, Big Data, Blockchain or the Internet of Things). There is currently a strong interest in secure distributed computation from governments and security organisations (in particular the National Institute of Standards and Technology, NIST), military, academia and industry. We are close to the stage where the secure distributed computation protocols can be applied to real-world security issues.

The main scientific challenges of the SANGRIA project are (1) to construct specific protocols that take into account practical constraints and prove them secure, (2) to implement them and to improve the efficiency of existing protocols significantly. The project aims at undertaking research in these two directions while combining research from cryptography, combinatorics and computer algebra. It is expected to impact central problems in secure distributed computation, while enriching the general landscape of cryptography.

9.3.8 ANR AGDE – Arithmetic and geometry of discrete groups

Participants: Aurel Page.

Project URL
Duration: 2021–2025

The AGDE ANR project is a young researcher ANR project led by Jean Raimbault.

Its main objects of study are groups of matrices with integer entries, as these are objects of interest in geometric group theory, number theory, differential geometry and topology. Its main objective is to study the properties that are common or different in various classes of such groups, with a particular focus on the asymptotic behaviour. The project focuses on torsion homology and regulators, and the classes of congruence groups, arithmetic but noncongruence groups, and thin subgroups. The development of computational methods is an important tool for the project.

10 Dissemination

Participants: Bill Allombert, Jared Asuncion, Razvan Barbulescu, Karim Belabas, Xavier Caruso, Guilhem Castagnos, Jean-Paul Cerri, Jean-Marc Couveignes, Andreas Enge, Jean Kieffer, Aurel Page, Alice Pellet-Mary, Damien Robert, Benjamin Wesolowski, Anne-Edgar Wilke.

10.1 Promoting scientific activities

10.1.1 Scientific events: organisation

PARI/GP Day 2021
B. Allombert and K. Belabas organised a PARI/GP Day to present the new features of the software. This online event replaced the usual PARI/GP workshop that was cancelled due to the pandemic.
Atelier francophone en ligne PARI/GP 2021b
B. Allombert, A. Page and A. Zekhnini organised a two-days online PARI/GP workshop to give an introduction to PARI/GP to the participants of the conference JATNA 2021 held in Oujda and to the students of the Afrimath network.

Member of conference programme committees A. Pellet-Mary was a member of the programme committee of the conferences Asiacrypt 2021, PKC 2022 and Eurocrypt 2022.

B. Wesolowski was a member of the programme committee of the conference PKC 2022.

J.-M. Couveignes is a member of the programme committee of the conference *A Tour of Arithmetic Geometry, conference in honour of Bas Edixhoven's 60th birthday*, Schiermonnikoog, April 2022.

10.1.2 Journal

Membership of editorial boards X. Caruso is an editor and one of the founders of the journal *Annales Henri Lebesgue*.

J.-M. Couveignes is a member of the editorial board (scientific committee) of the *Publications mathématiques de Besançon* since 2010 and of *Journal de Théorie des Nombres de Bordeaux* since 2020.

K. Belabas acts on the editorial board of *Journal de Théorie des Nombres de Bordeaux* since 2005 and of *Archiv der Mathematik* since 2006.

A. Enge is an editor of *Designs, Codes and Cryptography* since 2004.

10.1.3 Scientific expertise

K. Belabas is a member of the "conseil scientifique" of the Société Mathématique de France (second mandate).

X. Caruso is a member of the "conseil national des universités" (CNU) since 2021.

10.1.4 Research administration

Since January 2015, K. Belabas is vice-head of the Mathematics Institute (IMB). He also leads the computer science support service ("cellule informatique") of IMB and coordinates the participation of the institute in the regional computation cluster PlaFRIM.

Since September 2021, he is vice-head of the Unité de Formation Mathématiques et Interactions (UFMI)

He was an elected member of "commission de la recherche" in the academic senate of Université de Bordeaux from 2014 to 2021.

A. Enge is a member of the administrative council of the Société Arithmétique de Bordeaux, which edits the *Journal de théorie des nombres de Bordeaux* and supports number theoretic conferences.

G. Castagnos is responsible for the bachelor programme in mathematics and informatics.

J.-M. Couveignes is co-responsible for the Graduate Programme Numerics of the Université de Bordeaux.

J.-M. Couveignes was head of the *comité de visite, d'analyse et de recommandation de l'équipe Modélisation et Applications du LMNO de Caen* at the request of CNRS-INSMI and Université de Caen Normandie.

10.2 Teaching - Supervision - Juries

10.2.1 Graduate schools

X. Caruso, P. Molin and A. Page supervised the computer algebra software sessions in the 2021 JC2A Summer School. Both Sagemath and PARI/GP were presented to the participants (PhD students in number theory).

10.2.2 Teaching

- Master: G. Castagnos, *Cryptanalyse*, 60h, M2, Université de Bordeaux, France;
- Master: G. Castagnos, *Cryptologie avancée*, 30h, M2, Université de Bordeaux, France;
- Master: G. Castagnos, *Courbes elliptiques*, 30h, M2, Université de Bordeaux, France;
- Licence: G. Castagnos, *Arithmétique et Cryptologie*, 24h, L3, Université de Bordeaux, France

- Master : D. Robert, *Courbes elliptiques*, 60h, M2, Université de Bordeaux, France;
- Master: X. Caruso and J.-M. Couveignes, *Algorithmique arithmétique, introduction à l'algorithmique quantique*, 60h, M2, Université de Bordeaux, France;
- Master : K. Belabas, *Algèbre et calcul formel 1 et 2*, 91h, M2, Université de Bordeaux, France;
- Licence: K. Belabas, *Algorithmique mathématique 2*, TD, 35h, L3, Université de Bordeaux, France;
- Licence: K. Belabas, *Structures algébriques 1*, TD, 19h, L2, Université de Bordeaux, France;
- Licence : J.-P. Cerri, *Arithmétique et Cryptologie*, TD, 36h, L3, Université de Bordeaux, France;
- Licence : J.-P. Cerri, *Structures Algébriques 2*, TD, 35h, L3, Université de Bordeaux, France;
- Licence : J.-P. Cerri, *Topologie*, TD, 35h, L3, Université de Bordeaux, France;
- Master : J.-P. Cerri, *Cryptologie*, Cours-TD, 60h, M1, Université de Bordeaux, France;
- Licence, Master : J.-P. Cerri, 2 TER (L3, M1), Université de Bordeaux, France;
- Licence : J.-M. Couveignes, *Mathematics*, Cours-TD, 165h, Cycle préparatoire de Bordeaux, Université de Bordeaux, France;
- Licence: J. Kieffer, *Algorithmique Mathématique 2*, 32h, L3, Université de Bordeaux, France;
- Master : J. Asuncion, *Elliptic curves*, TD, 16h, M1, Universiteit Utrecht (Mastermath), Pays-Bas;
- Master: D. Robert, *Courbes elliptiques*, 30h, M2, Université de Bordeaux, France;
- Licence : A.-E. Wilke, *Outils mathématiques pour la biologie*, TD, 32h, Université de Bordeaux, France;
- Licence : A.-E. Wilke, *Coloration mathématique*, TD, 32h, Université de Bordeaux, France.

10.2.3 Supervision

- PhD in progress: Jared Asuncion, *Class fields of complex multiplication fields*, since September 2017, supervised by A. Enge and Marco Streng (Universiteit Leiden).
- PhD in progress: Élie Bouscatié, *Conception d'algorithmes de chiffrement cherchable*, since November 2020, supervised by Guilhem Castagnos
- PhD in progress: Amaury Durand, *Geometric Gabidulin codes*, since September 2019, supervised by Xavier Caruso
- PhD in progress: Raphaël Pagès, *Factorisation des opérateurs différentiels en caractéristique p*, since September 2020, supervised by Alin Bostan and Xavier Caruso
- PhD in progress: Anne-Edgar Wilke *Enumerating integral orbits of prehomogeneous representations*, since September 2019, supervised by K. Belabas.
- PhD in progress: Agathe Beaugrand, *Conception de systèmes cryptographiques utilisant des groupes de classes de corps quadratiques*, since September 2021, supervised by Guilhem Castagnos and Fabien Laguillaumie.
- PhD defended in 2021: Jean Kieffer, *Computing isogenies between abelian surfaces* [31], supervised by Damien Robert and Aurel Page
- PhD in progress: Abdoulaye Maiga, *Computing canonical lift of genus 2 hyperelliptic curves*, University Dakar, supervised by Djiby Sow, Abdoul Aziz Ciss and D. Robert.
- PhD defended in 2021: Élie Eid, *On isogeny calculation by solving p-adic differential equations* [30], Université de Rennes, supervised by Xavier Caruso and Reynald Lercier

10.2.4 Juries

- R. Barbulescu was part of the jury (3 members) of the oral admission exam in mathematics at ENS de Lyon (creation of original exercices and examination of approximately 85 candidates)
- K. Belabas has written a report for the doctoral dissertation by Aude Le Gluher, Université de Lorraine: *Symbolic computation and complexity analyses for number theory and cryptography*.
- X. Caruso was part of the jury of the doctoral dissertation of Luming Zhao, Université de Bordeaux: *Cohomologie galoisienne pour les corps p-adiques et (φ,τ)-modules*.
- X. Caruso was part of the jury of the doctoral dissertation of Abhinandan, Université de Bordeaux: *Finite height representations and syntomic complex*.
- X. Caruso and J.-M. Couveignes were part of the selection committee for a position of associate professor in the University of Toulouse.
- X. Caruso was part of the selection committee for a position of associate professor in the University of Limoges.
- G. Castagnos has written a report for the doctoral dissertation by Nagarjun Dwarakanath, Université Paris-Saclay: *Theoretical and practical contributions to homomorphic encryption*.
- G. Castagnos has written a report for the doctoral dissertation by Rémi Clarisse, Université Rennes 1: *Conception de courbes elliptiques et applications*.
- J.-M. Couveignes was part of the jury of the doctoral dissertation by Rémi Clarisse, Université Rennes 1: *Conception de courbes elliptiques et applications*.
- J.-M. Couveignes was part of the jury of the doctoral dissertation by Élie Eid, Université Rennes 1: *Computing isogenies between elliptic curves and curves of higher genus*.
- J.-M. Couveignes was part of the jury of the doctoral dissertation by Jean Kieffer, Université de Bordeaux: *Computing isogenies between abelian surfaces*.
- J.-M. Couveignes has written a report for the doctoral dissertation by Angelot Behajaina, Université de Caen Normandie: *Aspects commutatifs et non commutatifs de la théorie inverse de Galois*.
- J.-M. Couveignes has written a report for the doctoral dissertation by Abdoulaye Maiga, *Computing canonical lift of genus 2 hyperelliptic curves*, University Dakar.
- A. Enge was part of the jury of the habilitation degree of Damien Robert, Université de Bordeaux: *Efficient algorithms for abelian varieties and their moduli spaces*.
- D. Robert has written a report for the doctoral dissertation by Mathilde Chenu, LIX: *Supersingular Group Actions and Post-quantum Key Exchange*.

10.3 Popularization

10.3.1 Internal or external Inria responsibilities

X. Caruso and C. Ménini are leaders of the popularisation group at IMB (Institut de Mathématiques de Bordeaux).

R. Barbulescu is one of the organisers of concours Alkindi [1], which proposes interactive exercises of cryptography for students of 8th, 9th and 10th grade (French 4e, 3e and 2nde). Together with the Ministries of Education and of Defense, the contest is supported by Inria and Thalès. In 2020-2021 the contest had 47000 participants and M. le Ministre Blanquer took part in the award ceremony, organised online. Barbulescu had two roles: an administrative task (he was one of the three organisers) and a

[1] URL Alkindi

scientific role (he was one of six researchers in this function), which consists in translating the latest research results into exercises adapted for middle- and high-school students.

X. Caruso and R. Barbulescu are the two members of the regional organisation committee of Tournoi français des jeunes mathématiciennes et mathématiciens (TFJM) in Bordeaux[2]. B. Wesolowski and A. Pellet-Mary were jury members.

R. Barbulescu takes part in the action for central Africa of the NGO Animath[3]. In 2020-2021, the sanitary context required to replace our regular actions, workshops with students in Africa, with online activities. Several countries took part in Olympiade Francophone de mathématiques and others organised Concours Alkindi. Our role was administrative: contact and discuss with institutions such as the French ambassy in Romania or the Inspectorat général du Ministère de l'Éducation du Sénégal.

10.3.2 Articles and contents

X. Caruso wrote a webpage with several models of slide rules[4]. Some of them were built in the FabLab at the IUT of Gradignan and are now exhibited in the library of our Math Department.

11 Scientific production

11.1 Major publications

[1] R. Barbulescu and J. Ray. 'Numerical verification of the Cohen-Lenstra-Martinet heuristics and of Greenberg's p-rationality conjecture'. In: *Journal de Théorie des Nombres de Bordeaux* 32.1 (21st Aug. 2020), pp. 159–177. URL: https://hal.archives-ouvertes.fr/hal-01534050.

[2] E. Bayer-Fluckiger, J.-P. Cerri and J. Chaubert. 'Euclidean minima and central division algebras'. In: *International Journal of Number Theory* 5.7 (2009), pp. 1155–1168. URL: https://hal.archives-ouvertes.fr/hal-00282364.

[3] K. Belabas, M. Bhargava and C. Pomerance. 'Error estimates for the Davenport-Heilbronn theorems'. In: *Duke Mathematical Journal* 153.1 (2010), pp. 173–210. URL: http://projecteuclid.org/euclid.dmj/1272480934.

[4] X. Caruso, D. Roe and T. Vaccon. 'Tracking p-adic precision'. In: *LMS J. Comput. Math.* 17 (2014), pp. 274–294.

[5] G. Castagnos, F. Laguillaumie and I. Tucker. 'Practical Fully Secure Unrestricted Inner Product Functional Encryption modulo p'. In: *Advances in Cryptology – ASIACRYPT 2018, Part II*. Ed. by T. Peyrin and S. Galbraith. Vol. 11273. Lecture Notes in Computer Science. International Association for Cryptologic Research, 2018, pp. 733–764.

[6] H. Cohen and F. Strömberg. *Modular Forms: A Classical Approach*. Vol. 179. Graduate Studies in Mathematics. American Mathematical Society, 2017. URL: http://bookstore.ams.org/gsm-179/.

[7] J.-M. Couveignes and B. Edixhoven. *Computational aspects of modular forms and Galois representations*. Princeton University Press, 2011.

[8] K. De Boer, L. Ducas, A. Pellet-Mary and B. Wesolowski. 'Random Self-reducibility of Ideal-SVP via Arakelov Random Walks'. In: CRYPTO 2020. Santa Barbara, United States, 17th Aug. 2020. DOI: 10.1007/978-3-030-56880-1_9. URL: https://hal.archives-ouvertes.fr/hal-02513308.

[9] A. Enge, W. Hart and F. Johansson. 'Short addition sequences for theta functions'. In: *Journal of Integer Sequences* 18.2 (2018), pp. 1–34.

[10] D. Lubicz and D. Robert. 'Computing isogenies between abelian varieties'. In: *Compositio Mathematica* 148.05 (Sept. 2012), pp. 1483–1515. DOI: 10.1112/S0010437X12000243. URL: http://dx.doi.org/10.1112/S0010437X12000243.

[2] URL TJFM Bordeaux
[3] URL Animath
[4] URL Sliders

11.2 Publications of the year

International journals

[11] R. Barbulescu and S. Shinde. 'A classification of ECM-friendly families using modular curves'. In: *Mathematics of Computation* (1st Sept. 2021). URL: https://hal.archives-ouvertes.fr/hal-01822144.

[12] X. Caruso. 'A theory of residues for skew rational functions'. In: *Journal de l'École polytechnique — Mathématiques* 8 (2021), pp. 1159–1192. URL: https://hal.archives-ouvertes.fr/hal-02268790.

[13] X. Caruso, E. Eid and R. Lercier. 'Fast computation of elliptic curve isogenies in characteristic two'. In: *Journal of the London Mathematical Society* 104.4 (2021), pp. 1901–1929. DOI: 10.1112/jlms.12487. URL: https://hal.archives-ouvertes.fr/hal-02508825.

[14] R. Cramer, L. Ducas and B. Wesolowski. 'Mildly Short Vectors in Cyclotomic Ideal Lattices in Quantum Polynomial Time'. In: *Journal of the ACM (JACM)* 68.2 (6th Jan. 2021), pp. 1–26. DOI: 10.1145/3431725. URL: https://hal.archives-ouvertes.fr/hal-03102234.

[15] E. Friedman, F. Johansson and G. Ramirez-Raposo. 'The minimal Fried average entropy for higher-rank Cartan actions'. In: *Mathematics of Computation* 90.328 (2021), pp. 973–978. URL: https://hal.inria.fr/hal-02904336.

[16] R. Granger, T. Kleinjung, A. K. Lenstra, B. Wesolowski and J. Zumbrägel. 'Computation of a 30 750-Bit Binary Field Discrete Logarithm'. In: *Mathematics of Computation* 90.332 (2021). URL: https://hal.archives-ouvertes.fr/hal-02945361.

[17] M. Kirschmer, F. Narbonne, C. Ritzenthaler and D. Robert. 'Spanning the isogeny class of a power of an elliptic curve.' In: *Mathematics of Computation* 91.333 (2021), pp. 401–449. URL: https://hal.inria.fr/hal-02554714.

[18] T. Kleinjung and B. Wesolowski. 'Discrete logarithms in quasi-polynomial time in finite fields of fixed characteristic'. In: *Journal of the American Mathematical Society* (2021). DOI: 10.1090/jams/985. URL: https://hal.archives-ouvertes.fr/hal-03347994.

[19] C. Maire and A. Page. 'Codes from unit groups of division algebras over number fields'. In: *Mathematische Zeitschrift* (2021). DOI: 10.1007/s00209-020-02614-5. URL: https://hal.inria.fr/hal-01770396.

International peer-reviewed conferences

[20] E. Bouscatié, G. Castagnos and O. Sanders. 'Public Key Encryption with Flexible Pattern Matching'. In: Asiacrypt 2021, the 27th Annual International Conference on the Theory and Application of Cryptology and Information Security. Vol. 13093. Lecture Notes in Computer Science. Singapour (en ligne), Singapore: Springer International Publishing, 1st Dec. 2021, pp. 342–370. DOI: 10.1007/978-3-030-92068-5_12. URL: https://hal.inria.fr/hal-03466491.

[21] X. Caruso, T. Vaccon and T. Verron. 'On FGLM Algorithms with Tate Algebras'. In: International Symposium on Symbolic and Algebraic Computation — ISSAC 2021. Virtual event, Russia: ACM, 18th July 2021. URL: https://hal.archives-ouvertes.fr/hal-03133590.

[22] E. Eid. 'Fast computation of hyperelliptic curve isogenies in odd characteristic'. In: International Symposium on Symbolic and Algebraic Computation — ISSAC 2021. Virtual event, Russia: ACM, 2021, pp. 131–138. URL: https://hal.archives-ouvertes.fr/hal-02948514.

[23] F. Johansson. 'Calcium: computing in exact real and complex fields'. In: ISSAC 2021 - International Symposium on Symbolic and Algebraic Computation. Saint-Petersbourg / Virtual, Russia: ACM, 2021, pp. 225–232. DOI: 10.1145/3452143.3465513. URL: https://hal.inria.fr/hal-02986375.

[24] A. Maiga and D. Robert. 'Computing the 2-adic Canonical Lift of Genus 2 Curves'. In: ICMC 2021 - 7th International Conference on Mathematics and Computing. Shibpur / Virtual, India, 2nd Mar. 2021. URL: https://hal.inria.fr/hal-03119147.

[25] R. Pagès. 'Computing Characteristic Polynomials of p-Curvatures in Average Polynomial Time'. In: ISSAC 2021 - International Symposium on Symbolic and Algebraic Computation. Saint-Petersbourg / Virtual, Russia: ACM, 2021, pp. 329–336. DOI: 10.1145/3452143.3465524. URL: https://hal.archives-ouvertes.fr/hal-03270585.

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

[27] S. A. K. Thyagarajan, G. Castagnos, F. Laguillaumie and G. Malavolta. 'Efficient CCA Timed Commitments in Class Groups'. In: CCS 2021 - ACM SIGSAC Conference on Computer and Communications Security. Seoul (online), South Korea, 12th Nov. 2021, pp. 2663–2684. DOI: 10.1145/3460120.3484773. URL: https://hal.inria.fr/hal-03466495.

[28] B. Wesolowski. 'The supersingular isogeny path and endomorphism ring problems are equivalent'. In: FOCS 2021 - 62nd Annual IEEE Symposium on Foundations of Computer Science. Denver, Colorado, United States, 7th Feb. 2022. URL: https://hal.archives-ouvertes.fr/hal-03340899.

Scientific books

[29] K. Belabas and H. Cohen. *Numerical Algorithms for Number Theory*. Vol. 254. Mathematical Surveys and Monographs. American Mathematical Society, 23rd June 2021. DOI: 10.1090/surv/254. URL: https://hal.archives-ouvertes.fr/hal-03500576.

Doctoral dissertations and habilitation theses

[30] E. Eid. 'On isogeny calculation by solving p-adic differential equations'. Université Rennes 1, 22nd June 2021. URL: https://tel.archives-ouvertes.fr/tel-03337021.

[31] J. Kieffer. 'Higher-dimensional modular equations, applications to isogeny computations and point counting'. Université de Bordeaux, 13th July 2021. URL: https://tel.archives-ouvertes.fr/tel-03346032.

[32] D. Robert. 'Efficient algorithms for abelian varieties and their moduli spaces'. Université de Bordeaux (UB), Mar. 2021. URL: https://hal.archives-ouvertes.fr/tel-03498268.

Reports & preprints

[33] J. Asuncion. *Computing the Hilbert Class Fields of Quartic CM Fields Using Complex Multiplication*. 27th Apr. 2021. URL: https://hal.inria.fr/hal-03210279.

[34] R. Barbulescu. *(Non)practicabilité de l'algorithme classique-quantique de factorisation des entiers*. Institut de mathématiques de Bordeaux, 1st Dec. 2021. URL: https://hal.archives-ouvertes.fr/hal-03483274.

[35] R. Barbulescu. *Rigorous time bound for factoring with elliptic curves*. 17th Dec. 2021. URL: https://hal.archives-ouvertes.fr/hal-03485435.

[36] J.-F. Biasse, C. Fieker, T. Hofmann and A. Page. *Norm relations and computational problems in number fields*. 14th July 2021. URL: https://hal.inria.fr/hal-02497890.

[37] X. Caruso. *Where are the zeroes of a random p-adic polynomial?* Oct. 2021. URL: https://hal.archives-ouvertes.fr/hal-02557280.

[38] X. Caruso, A. David and A. Mézard. *Combinatorics of Serre weights in the potentially Barsotti-Tate setting*. 5th Nov. 2021. URL: https://hal-cnrs.archives-ouvertes.fr/hal-03221168.

[39] X. Caruso and A. Durand. *Duals of linearized Reed-Solomon codes*. 22nd Oct. 2021. URL: https://hal.archives-ouvertes.fr/hal-03395402.

[40] X. Caruso, M. Mezzarobba, N. Takayama and T. Vaccon. *Fast evaluation of some p-adic transcendental functions*. 16th June 2021. URL: https://hal-cnrs.archives-ouvertes.fr/hal-03263044.

[41] H. Cohen. *Computing L-Functions of Quadratic Characters at Negative Integers*. 2021. URL: https://hal.inria.fr/hal-03139244.

[42] H. Cohen and J. Guillera. *Rational Hypergeometric Ramanujan Identities for $1/\pi^c$: Survey and Generalizations*. 2021. URL: https://hal.inria.fr/hal-03139250.

[43] J.-M. Couveignes and T. Ezome. *The equivariant complexity of multiplication in finite field extensions*. 31st Oct. 2021. URL: https://hal.archives-ouvertes.fr/hal-03410146.

[44] E. Eid. *Computing isogenies between Jacobians of hyperelliptic curves of arbitrary genus via differential equations*. 2021. URL: https://hal.archives-ouvertes.fr/hal-03142205.

[45] F. Johansson. *Arbitrary-precision computation of the gamma function*. 16th Sept. 2021. URL: https://hal.inria.fr/hal-03346642.

[46] F. Johansson. *Rapid computation of special values of Dirichlet L-functions*. 20th Oct. 2021. URL: https://hal.inria.fr/hal-03386620.

[47] J. Kieffer. *Degree and height estimates for modular equations on PEL Shimura varieties*. 3rd May 2021. URL: https://hal.archives-ouvertes.fr/hal-02436057.

[48] J. Kieffer. *Upper bounds on the heights of polynomials and rational fractions from their values*. 3rd May 2021. URL: https://hal.archives-ouvertes.fr/hal-03226568.

[49] D. Lubicz and D. Robert. *Linear representation of endomorphisms of Kummer varieties*. 21st Apr. 2021. URL: https://hal.archives-ouvertes.fr/hal-03204365.

[50] B. Wesolowski. *A proof of time or knowledge*. 15th Oct. 2021. URL: https://hal.archives-ouvertes.fr/hal-03380471.

11.3 Cited publications

[51] K. Belabas. 'L'algorithmique de la théorie algébrique des nombres'. In: *Théorie algorithmique des nombres et équations diophantiennes*. Ed. by N. Berline, A. Plagne and C. Sabbah. 2005, pp. 85–155.

[52] J.-P. Cerri. 'Inhomogeneous and Euclidean spectra of number fields with unit rank strictly greater than 1'. In: *J. Reine Angew. Math.* 592 (2006), pp. 49–62.

[53] J.-P. Cerri. 'Spectres euclidiens et inhomogènes des corps de nombres'. Thèse de doctorat. IECN, Université Henri Poincaré, Nancy, 2005. URL: http://tel.archives-ouvertes.fr/tel-00011151/en/.

[54] D. Charles, E. Goren and K. Lauter. 'Cryptographic Hash Functions from Expander Graphs'. In: *Journal of Cryptology* 22.1 (2009), pp. 93–113.

[55] H. Cohen and P. Stevenhagen. 'Computational class field theory'. In: *Algorithmic Number Theory — Lattices, Number Fields, Curves and Cryptography*. Ed. by J. Buhler and P. Stevenhagen. Vol. 44. MSRI Publications. Cambridge University Press, 2008.

[56] A. Enge. 'Courbes algébriques et cryptologie'. Habilitation à diriger des recherches. Paris 7: Université Denis Diderot, 2007. URL: http://tel.archives-ouvertes.fr/tel-00382535/en/.

[57] A. Rostovtsev and A. Stolbunov. 'Public-key cryptosystem based on isogenies'. Preprint, Cryptology ePrint Archive 2006/145. 2006. URL: http://eprint.iacr.org/2006/145/.