RESEARCH CENTRE

Inria Center at the University of Bordeaux

IN PARTNERSHIP WITH:

Université de Bordeaux, CNRS

2022
ACTIVITY REPORT

Team
LFANT

Lithe and fast algorithmic number theory

Inria teams are typically groups of researchers working on the definition of a common project, and objectives, with the goal to arrive at the creation of a project-team. Such project-teams may include other partners (universities or research institutions)

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

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Algorithmics, Computer Algebra and Cryptology

Contents

Team LFANT

Creation of the Team: 2022 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 Barbulescu [CNRS, Researcher]
- Xavier Caruso [CNRS, Senior Researcher, HDR]
- Fredrik Johansson [INRIA, Researcher]
- Aurel Page [INRIA, Researcher]
- Alice Pellet Mary [CNRS, Researcher]
- Damien Olivier Robert [INRIA, Researcher, HDR]
- Benjamin Wesolowski [CNRS, Researcher]

Faculty Members

- Karim Belabas [UNIV BORDEAUX, Professor, HDR]
- Guilhem Castagnos [UNIV BORDEAUX, Associate Professor, HDR]
- Jean Cerri [UNIV BORDEAUX, Associate Professor]
- Henri Cohen [UNIV BORDEAUX, HDR]
- Jean-Marc Couveignes [UNIV BORDEAUX, Professor, HDR]

Post-Doctoral Fellows

- Leo Poyeton [ENS DE LYON]
- Wessel Van Woerden [UNIV BORDEAUX, from Nov 2022]

PhD Students

- Jared Asuncion [Universiteit Leiden, until May 2022]
- Agathe Beaugrand [UNIV BORDEAUX]
- Elie Bouscatie [ORANGE, CIFRE]
- Pierrick Dartois [INRIA, from Oct 2022]
- Amaury Durand [UNIV BORDEAUX]
- Fabrice Etienne [ENS RENNES, from Aug 2022]
- Jean Gasnier [UNIV BORDEAUX, from Oct 2022]
- Raphaël Pagès [UNIV BORDEAUX]
- Nicolas Sarkis [UNIV BORDEAUX, from Oct 2022]
- Anne-Edgar Wilke [INRIA]

Technical Staff

- Bill Allombert [CNRS, Engineer]

Administrative Assistants

- Sabrina Duthil [INRIA]
- Joelle Rodrigues [INRIA]

External Collaborator

- Luca De Feo [IBM RESEARCH EUROPE, HDR]

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, Fabrice Etienne, Fredrik Johansson, Aurel Page, Anne-Edgar Wilke.

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 [45] 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, Pierrick Dartois, Luca De Feo, Andreas Enge, Jean Gasnier, Jean Kieffer, Alice Pellet-Mary, Damien Robert, Nicolas Sarkis, Benjamin Wesolowski.

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.

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 [50], for more background material, see [49]. 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 [47, 46].

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 [48] and encryption [51]. 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, Karim Belabas and Henri Cohen have been awarded the 2021 ACM/SIGSAM Richard Dimick Jenks Memorial Prize for Excellence in Software Engineering applied to Computer Algebra for the Pari/GP computer algebra system, see the announcement. The prize has been given at ISSAC 2022.

5.2 Breaking a post-quantum cryptosystem

D. Robert has described a polynomial time algorithm for breaking SIDH in [38]. The system was the main contender for isogeny based key exchange to withstand the threat of a potential quantum computer, submitted to the NIST competition for a new standard. D. Robert's work completely breaks the cryptosystem already in a classical, non quantum setting, by building on years of mathematical and algorithmic studies of isogenies of higher dimensional abelian varieties.

5.3 Defenses

Jared Asuncion has defended his doctoral degree with a thesis entitled *Complex multiplication constructions of abelian extensions of quartic fields* [31].

Amaury Durand has defended his doctoral degree with a thesis entitled *Duaux des codes de Reed-Solomon linéarisés; résidus de polynômes tordus.*

Abdoulaye Maiga has defended in June his doctoral degree with a thesis entitled *Relèvement canonique de surfaces abéliennes.*

5.4 Institutional life

The team wishes to thank the Commission d'Évaluation for its outstanding efforts, in 2022 and previous years, in defending the interests of the research community, keeping us thoroughly informed about topics relevant to the scientific life at INRIA, and upholding the moral and intellectual values we are collectively proud of and which define our institute.

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: Aurel Page

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: Changes in version 1.3.1, released in December 2022: - Bug fix: It is again possible to include mpc.h without including stdio.h.

Changes in version 1.3.0 ("Ipomoea batatas"), released in December 2022: - New function: mpc_agm - New rounding modes "away from zero", indicated by the letter "A" and corresponding to MPFR_RNDA on the designated real or imaginary part. - New experimental ball arithmetic. - New experimental function: mpc_eta_fund - Bug fixes: - mpc_asin for asin(z) with small |Re(z)| and tiny |Im(z)| - mpc_pow_fr: sign of zero part of result when the base has up to sign the same real and imaginary part, and the exponent is an even positive integer - mpc_fma: the returned 'int' value was incorrect in some cases (indicating whether the rounded real/imaginary parts were smaller/equal/greater than the exact values), but the computed complex value was correct. - Remove the unmaintained Makefile.vc, build files for Visual Studio can be found at https://github.com/BrianGladman/mpc .

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 Olivier Robert

Participants: Damien Olivier 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 0.4 ("Fitzebohnen"): - increase minimal version number for mpfrcx to 0.6.3 and for pari to 2.11. - add decomposition of the class field into a tower of prime degree extensions - add a fastECPP implementation, including a version for MPI

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.

Release Contributions: Changes in version 1.1.0 of 2022-07-20: * Implement N-systems, and use 1-systems. * Adapt coefficient recognition to FPLLL-5.4.2.

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

Contact: Emmanuel Thome

Participants: Andreas Enge, Emmanuel Thome, 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 Olivier 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.

Release Contributions: Changes in version 0.1.1: - Wrapped functions acb_overlaps, acb_contains, acb_sqrt, acb_pow, acb_agm, acb_sinh, acb_cosh, acb_elliptic_k, acb_elliptic_e and acb_hypgeom_2f1.

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 contributes the improvement and maintenance of the graph module and its 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 Cerri

Participants: Jean 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

6.1.17 Calcium

Name: Calcium

Keywords: Computer algebra, Numerical analysis

Functional Description: C library for exact computation with real and complex numbers

Contact: Fredrik Johansson

6.1.18 quartic

Keyword: Quartic number fields

Functional Description: The purpose of this program is to compute tables of primitive quartic number fields whose absolute discriminant is bounded by some given constant.

Release Contributions: Initial version.

Contact: Anne-Edgar Wilke

6.1.19 BICYCL

Name: BICYCL Implements CryptographY in CLass groups

Keywords: Cryptography, Number theory

Functional Description: BICYCL is a C++ library that implements arithmetic in the ideal class groups of imaginary quadratic fields, together with a set of cryptographic primitives based on class groups.

URL: https://crypto.lirmm.net/bicycl/

Contact: Guilhem Castagnos

Partner: Université de Montpellier

7 New results

7.1 Coding theory and cryptology

Participants: Razvan Barbulescu, Xavier Caruso, Guilhem Castagnos, Amaury Durand, 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 found that the DLP is much easier than previously believed in an important family: finite fields of *small characteristic*, where 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 [21], 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 $(pn)^{2\log_2(n)+O(1)}$.

Functional Encryption Inner product functional encryption (IPFE) is a primitive which produces, from a master secret key, decryption keys sk_k associated to vectors k over some specified base ring. Decrypting an encryption of vector m with sk_k only reveals $\langle k, m \rangle$. Benhamouda et al. provided a generic construction for CCA-secure IPFE from projective hash functions (PHFs), unfortunately their security reduction suffers an exponential loss. Their only instantiation capable of decrypting inner products of large sizes, which relies on the decisional composite residuosity (DCR) assumption, is impractical due to the large size of ciphertexts, decryption keys, and the prohibitively low speed of the scheme. In [17], G. Castagnos, F. Laguillaumie and I. Tucker develop a new approach to proving CCA security. Their constructions maintain the genericity of the previous work, while their security proof relaxes the requirements on the underlying PHFs and gains in reduction tightness. They instantiate these constructions from the DCR assumption, an assumption in class groups (HSM) and the decision Diffie Hellman (DDH) assumption. The CCA-secure constructions from DCR and HSM are the first such schemes to efficiently decrypt inner products of large size, improving by *multiple orders of magnitude* upon previous work. A single-core C implementation of these schemes shows that, for a 112 bit security, and 100−dimensional vectors, the previous DCR-based scheme takes 1h20min to encrypt and over 5min to decrypt, whereas the *slowest* proposed scheme takes 5.2s to encrypt and 0.5s to decrypt. Similarly a ciphertext for the previous scheme is of 283MB; those of the proposed HSM-based scheme are of 30kB.

Linearly Homomorphic Encryption In [24], accepted at the ASIACRYPT'22 conference, Castagnos, Laguillaumie and Tucker provide the first threshold linearly homomorphic encryption whose message space is $\mathbf{Z}/2^k\mathbf{Z}$ for any k. It is inspired by Castagnos and Laguillaumie's encryption scheme from RSA 2015, but works with a class group of discriminant whose factorisation is unknown. Its natural structure *à la* ElGamal makes it possible to distribute the decryption among servers using linear integer secret sharing, allowing any access structure for the decryption policy. Furthermore its efficiency and its flexibility on the choice of the message space make it a good candidate for applications to multiparty computation.

Implementation of Class Group based Cryptography In [33], Bouvier, Castagnos, Imbert and Laguillaumie introduce BICYCL, an Open Source C++ library that implements arithmetic in the ideal class groups of imaginary quadratic fields, together with a set of cryptographic primitives based on class groups. It is available here under the GNU General Public License version 3 or any later version. It provides significant speed-ups on the implementation of the arithmetic of class groups. Concerning cryptographic applications, BICYCL is orders of magnitude faster than any previous implementation of the Castagnos–Laguillaumie linearly homomorphic encryption scheme, making it faster than Paillier's encryption scheme at any security level. Linearly homomorphic encryption is the core of many multi-party computation protocols, sometimes involving a huge number of encryptions and homomorphic evaluations: class group based protocols become the best solution in terms of bandwidth and computational efficiency to rely upon.

Multi-party computation Due to their use in crypto-currencies, threshold ECDSA signatures have received much attention in recent years. Though efficient solutions now exist both for the two party, and the full threshold scenario, there is still much room for improvement, be it in terms of protocol functionality, strengthening security or further optimising efficiency.

In the past few months, a range of protocols have been published, allowing for a non interactive – and hence extremely efficient – signing protocol; providing new features, such as identifiable aborts (parties can be held accountable if they cause the protocol to fail), fairness in the honest majority setting (all parties receive output or nobody does) and other properties. In some cases, security is proven in the strong simulation based model. In [16], G. Castagnos, D. Catalano, F. Laguillaumie, F. Savasta and I. Tucker combine ideas from the aforementioned articles with the suggestion of Castagnos *et al.* (PKC 2020) to use the class group based CL framework so as to drastically reduce bandwidth consumption.

Building upon this latter protocol they present a new, maliciously secure, full threshold ECDSA protocol that achieves additional features without sacrificing efficiency. Their most basic protocol boasts a non interactive signature algorithm and identifiable aborts. They also propose a more advanced variant that achieves adaptive security (for the n-out-of-n case) and proactive security. The resulting constructions improve upon state of the art Paillier's based realisations achieving similar goals by up to a 10 factor in bandwidth consumption.

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 [32] R. Barbulescu and F. Jouve prove 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 they prove that a recent conjecture of Pollack's implies the correctness in the general case.

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 [22], K. Boudgoust, E. Gachon and A. Pellet-Mary show that some algebraic lattices with a lot of symmetries (namely, ideal lattices stabilised by field automorphisms) can lead to easier algorithmic problems than non structured lattices. They also demonstrate this weakness by implementing an attack on some cryptographic scheme using these lattices with too much structure. In [26], J. Felderhoff, A. Pellet-Mary and D. Stehlé extend a result from last year by A. Pellet-Mary and D. Stehlé on the algorithmic problem NTRU (used in many post-quantum cryptographic primitives). The previous work proved a lower bound on the hardness of NTRU (by reducing a more standard lattice problem to NTRU), whereas this new result shows an equivalence between NTRU and another (more standard) problem.

Isogeny-based cryptography is another popular candidate for post-quantum cryptography which relies on the presumed hardness of computing isogenies between elliptic curves. The cryptosystems of this family actually rely on a variety of computational assumptions which do not trivially relate to each other. In [30], B. Wesolowski proves the equivalence of two of the most fundamental problems: the supersingular isogeny path problem, and the supersingular endomorphism ring problem (assuming the generalised Riemann hypothesis). In [29], he then shows how these problems relate to group actions, exposing a hierarchy of computational problems. These results notably imply that the security of the CSIDH cryptosystem is equivalent to some specialisation of the endomorphism ring problem. In [25], W. Castryck, M. Houben, F. Vercauteren and B. Wesolowski show that the decisional variants of some of these problems are often easy to solve.

Finally, in the preprint [41], B. Wesolowski shows that contrary to previous belief, analogs of isogeny-based cryptosystems using Drinfeld modules are insecure.

Coding theory. In [15], X. Caruso et A. Durand develop a theory of residues for Ore rational functions in the differential case and use it to give a description of the duals of linearised Reed-Solomon codes. Their construction shows in particular that, under some assumptions on the base field, the class of linearised Reed-Solomon codes is stable under duality.

7.2 Number fields and symbolic computation

Participants: Xavier Caruso, Aurel Page, Jean Kieffer, Raphaël Pagès, Anne-Edgar Wilke.

Given a polynomial P of degree D with integer 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 [20] Kieffer explains how, when given more evaluation 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.

The paper [12] has been published, in which A. Page and his coauthors 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).

In [28], A. Page and P. Molin describe algorithms to represent and compute groups of Hecke characters of a number field. They obtain the whole family of such characters, including transcendental ones. They also show how to isolate the algebraic characters, which are of particular interest in number theory. These results have been implemented in PARI/GP, and they illustrate their work with a variety of examples using this implementation, in particular showing the interactions with modular forms, L-functions and abelian varieties.

A.-E. Wilke has written a program [44] whose purpose is to compute tables of primitive quartic number fields with bounded absolute discriminant. The underlying theoretical tool is Bhargava's bijection between such fields and certain classes of pairs of ternary quadratic forms with integer coefficients. This program has been used to compute the complete list of all primitive quartic number fields of absolute discriminant at most 10^9, which is available here.

7.3 Modular forms and L-functions

Participants: Razvan Barbulescu, Karim Belabas, Henri Cohen.

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 [34], H. Cohen shows how to obtain infinitely many continued fractions for certain $\mathbb{Z}$-linear combinations of zeta and L-values. While the three different suggested methods are completely elementary, they lead to a wealth of examples, actually a number of infinite families.

7.4 Complex multiplication and isogenies of abelian varieties

Participants: Jean-Marc Couveignes, Tony Ezome, Jean Kieffer, Abdoulaye Maiga, Damien Robert, Benjamin Wesolowski.

In [35], 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.

In [18], 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 [19], J. Kieffer shows that the sign choices made in Dupont's algorithm to evaluate genus 2 theta constants in quasi-linear time in the precision are indeed correct. This gives a positive answer to a question raised by Dupont in his 2006 thesis, and lifts one of the heuristic that Dupont's algorithm uses.

In [30], 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 [27], accepted for publication at the ANTS 2022 conference, D. Lubicz and D. Robert give new change of level formulas between theta functions with a quasi-linear time complexity. As an application, they derive an algorithm to compute ℓ-isogenies in the theta model in time $O(\ell^g)$ for all odd l. This improves their previous algorithm, which was of complexity $O(\ell^{2g})$ when l was a sum of four squares.

In [37], A. Maiga and D. Robert improve the dependency on p of Satoh's canonical lift algorithm. Notably they prove that one can lift an ordinary elliptic curve $E/\mathbb{F}_{p^n}$ to p-adic precision m in time $\tilde{O}(nmp)$. Satoh's original algorithm was in $\tilde{O}(nmp^2 + p^3)$. In particular the new method gives a point counting algorithm in time $\tilde{O}(n^2 p)$. And in [40] they describe a method to compute the canonical lift of an abelian surface in odd characteristic using modular polynomials.

In [38], D. Robert gives a polynomial time algorithm to break SIDH in all cases. This result extends previous results by Castryck–Decru which heuristically broke SIDH in polynomial time when the endomorphism ring of the starting curve was known, and of Maino–Martindale, who suggested a subexponential attack.

In [39], D. Robert shows that any isogeny on an abelian variety admits a representation taking polylogarithmic space and allowing evaluation in polylogarithmic time.

7.5 Geometry and arithmetic over the p-adics

Participants: Xavier Caruso.

In [23], continuing their work on the computation of Gröbner bases over Tate algebras, X. Caruso, T. Vaccon and T. Verron study ideals spanned by polynomials or overconvergent series in a Tate algebra. They prove that ideals which are spanned by polynomials admit a Tate Gröbner basis made of polynomials, and propose an algorithm for computing it. As a result, the size of the output of this algorithm grows linearly with the precision. They also prove the existence of a universal analytic Gröbner basis for polynomial ideals in Tate algebras, compatible with all convergence radii.

In [13], 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.

In [14], X. Caruso, A. David and A. Mézard propose some evidences towards a new type of Langlands correspondence (of combinatorial nature) which they call the 1-adic Langlands correspondence.

7.6 Multiprecision arithmetic

Participants: Fredrik Johansson.

In [36], F. Johansson presents a new algorithm for calculating elementary functions at high precision, achieving a speed-up of roughly a factor of 2 at precisions above 1000 digits. The method is implemented in the latest version of Arb.

7.7 Convexity and plurisubharmonicity

Participants: Anne-Edgar Wilke.

In [42], A.-E. Wilke first tries to make the known analogy between convexity and plurisubharmonicity more precise. Then he introduces a notion of strict plurisubharmonicity analogous to strict convexity, and he shows how this notion can be used to study the strong maximum modulus principle in Banach spaces. As an application, he defines a notion of L^p direct integral of a family of Banach spaces, which includes at once Bochner L^p spaces, ℓ^p direct sums and Hilbert direct integrals, and he shows that under suitable hypotheses, when $p < \infty$, an L^p direct integral satisfies the strong maximum modulus principle if and only if almost all members of the family do. This statement can be considered as a rewording of several known results, but the notion of strict plurisubharmonicity yields a new proof, which has the advantage of being short, enlightening and unified.

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 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. This projects is managed by researchers from Bordeaux, Besançon and Franceville (Gabon). 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. In April 2022 a workshop has been organized at the École Normale Supérieure de Libreville during 3 weeks for PhD student. In December 2021 a research school has been organized at the Institut de Mathématiques et Sciences Physiques du Bénin during 2 weeks (30 participants). In Decembre 2022 a research school has been organized in Libreville during 2 weeks (50 participants).

9.1.2 Visits of international scientists

The following international researchers have given a presentation in the Lfant team seminar:

- Céline Maistret (University of Bristol, UK)
- Elisa Lorenzo Garcia (Université de Neuchâtel, Switzerland)
- Andreas Pieper (Universität Ulm, Germany)
- Lassina Dembélé (King's College London, UK)
- Sergey Yurkevich (University of Vienna, Austria)
- Wessel van Woerden (CWI Amsterdam, Netherlands)
- Michael Monagan (Simon Fraser University, Vancouver, Canada)

9.2 National initiatives

9.2.1 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.

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

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

ANR URL
Project URL
Duration: 2017–2022

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.

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

Participants: Xavier Caruso, Jean-Marc Couveignes.

ANR URL
Duration: 2018–2023

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.

9.2.4 ANR CIAO – Cryptography, Isogenies and Abelian varieties Overwhelming

Participants: Bill Allombert, Jean-Marc Couveignes, Pierrick Dartois, Jean Gasnier, Aurel Page, Damien Robert, Nicolas Sarkis, Benjamin Wesolowski.

ANR URL
Duration: 2019–2024

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.

9.2.5 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.

9.2.6 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.

9.2.7 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.

9.2.8 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, Razvan Barbulescu, Karim Belabas, Xavier Caruso, Guilhem Castagnos, Jean-Paul Cerri, Jean-Marc Couveignes, Fredrik Johansson, Aurel Page, Alice Pellet-Mary, Damien Robert, Benjamin Wesolowski.

10.1 Promoting scientific activities

10.1.1 Scientific events: organisation

PARI/GP Atelier 2022
B. Allombert and K. Belabas organised the annual PARI/GP Workshop in Besançon to present the new features of the software and discuss future directions with the community.
Atelier francophone hybride PARI/GP 2022b
B. Allombert, A. Page and A. Zekhnini organised a two-days hybrid PARI/GP workshop to give an introduction to PARI/GP to the participants of the conference JATNA 2022 held in Oujda.

Member of conference programme committees J.-M. Couveignes was 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.

A. Pellet-Mary and B. Wesolowski were members of the programme committees of the conferences ANTS 2022 and PKC 2023.

X. Caruso was Publicity Chair at the conference ISSAC 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*. He is a member of the editorial board (scientific committee) of *Journal de Théorie des Nombres de Bordeaux* since 2022.

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 *Archiv der Mathematik* since 2006.

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

A. Page is an associate editor of the LMFDB since 2022.

10.1.3 Invited talks

A. Page gave an online invited talk at the conference Arithmetic groups and 3-manifolds (Bonn, MPIM) initially scheduled for March 2020 but rescheduled to May 2022 because of the pandemic.

F. Johansson gave an invited plenary talk at the Fifteenth Algorithmic Number Theory Symposium, ANTS-XV at the University of Bristol.

F. Johansson gave invited talks at the online conferences Big Data in Pure Mathematics 2022 and Global Virtual Sage Days 112.358.

10.1.4 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.

X. Caruso was president of the HCERES evaluation of Institut de Mathématiques de Marseille.

A. Enge took part in the HCERES evaluation of Institut de Mathématiques de Toulon.

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.

10.1.5 Research administration

Up to March 2022, K. Belabas was vice-head of the Mathematics Institute (IMB); he also led the IT support service (“cellule informatique”) of IMB. X. Caruso took his place in March 2022.

Up to March 2022, K. Belabas was vice-head of the Unité de Formation Mathématiques et Interactions (UFMI).

Since March 2022, K. Belabas is vice-president of the Université de Bordeaux, in charge of digital policies, including privacy, security and data management. He coordinates the 59M€ INFRANUM project for the 2021–2027 CPER financing mutualised numerical infrastructures for all universities and engineering schools of the Nouvelle Aquitaine region.

A. Enge and A. Page are members 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.

R. Barbulescu is a member of the Laboratory council of the IMB since september 2022.

10.2 Teaching - Supervision - Juries

10.2.1 Graduate schools

A. Pellet-Mary gave a course about lattice-based cryptography at a summer school in Budapest (master and PhD students).

A. Page gave a course about computational mathematics and Pari/GP at the SuSAAN Summer School in the Nesin Math Village (Izmir, Turkey).

At the Cogent Summer School in Grenoble, A. Page gave a mini-course about arithmetic groups in low rank and number theory, and B. Allombert gave a Pari/GP mini-course.

10.2.2 Teaching

- Master : A. Pellet-Mary, *Algèbre et calcul formel 1 et 2*, 36h, M2, Université de Bordeaux, France;
- 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*, 64h, M2, Université de Bordeaux, France;
- Licence : J.-P. Cerri, *Mathématiques générales*, CI, 35h, L1, Université de Bordeaux, France;
- Licence : J.-P. Cerri, *Structures Algébriques 1*, TD, 51h, L2, Université de Bordeaux, France;
- Licence : J.-P. Cerri, *Structures Algébriques 2*, TD, 35h, L3, Université de Bordeaux, France;
- Master : J.-P. Cerri, *Cryptologie*, Cours-TD, 60h, 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;
- EDMI doctoral school: R. Barbulescu, *Tournoi français des jeunes mathématiciennes et mathématiciens, création et évaluation des sujets*, 12h, Université de Bordeaux, France;

10.2.3 Supervision

- PhD: Jared Asuncion, *Class fields of complex multiplication fields*, supervised by A. Enge and Marco Streng (Universiteit Leiden), defended in May 2022.
- PhD: Amaury Durand, *Geometric Gabidulin codes*, supervised by X. Caruso, defended in December 2022.
- PhD: Abdoulaye Maiga, *Computing canonical lift of genus 2 hyperelliptic curves*, University Dakar, supervised by Djiby Sow, Abdoul Aziz Ciss and D. Robert, defended in 2022
- PhD in progress: Élie Bouscatié, *Conception d'algorithmes de chiffrement cherchable*, since November 2020, supervised by G. Castagnos
- PhD in progress: Raphaël Pagès, *Factorisation des opérateurs différentiels en caractéristique p*, since September 2020, supervised by A. Bostan and X. 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 in progress: Fabrice Étienne, *Techniques d'induction pour l'algorithmique des représentations galoisiennes*, since September 2022, supervised by Aurel Page.
- PhD in progress: Nicolas Sarkis, *Recherche de courbes planes de genre 2 adaptée à la factorisation des entiers*, since September 2022, supervised by Razvan Barbulescu and Damien Robert.
- PhD in progress: Pierrick Dartois *Improvement and security analysys of isogeny-based cryptographic schemes*, since September 2022, supervised by Damien Robert and Benjamin Wesolowski.
- PhD in progress: Jean Gasnier, *Algorithmique des isogénies et applications*, since October 2022, supervised by Jean-Marc Couveignes.

10.2.4 Juries

- A. Page took part in the INRIA hiring committee for Chargés de recherche and INRIA Starting Faculty positions in Bordeaux.
- R. Barbulescu was a member 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 has written a report for the doctoral dissertation by Christophe Levrat, Sorbonne université: *Calcul effectif de la cohomologie des faisceaux constructibles sur le site étale d'une courbe.*
- J.-M. Couveignes was part of the jury of the doctoral dissertation by Leonardo Colo, Université Aix-Marseille: *Oriented supersingular elliptic curves and class group actions.*
- J.-M. Couveignes was part of the jury of the doctoral dissertation by Bastien Pacifico, Université Aix-Marseille: *Construction polynomiale d'algorithmes de multiplication de type Chudnovsky de complexité bilinéaire linéaire.*
- 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.
- J.-M. Couveignes has written a report for the doctoral dissertation by Ali Issa, *Sur l'uniformité différentielle des polynômes sur les corps finis de caractéristique paire*, Université de Toulon.
- D. Robert has written a report for the doctoral dissertation by Salamithe Tsakou, Université de Picardie Jules Verne *Algebraic cryptanalysis of hyperelliptic curves based systems.*

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 2021-2022 the contest had 57000 participants from 800 middle and high schools. R. Barbulescu had two roles: an administrative task (he was one of the three organisers) and a 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. D. Robert invited the local Alkindi laureates to visit IMB and Inria Bordeaux to discuss with researchers and also gave a talk about cryptography.

R. Barbulescu is one of the four members of the regional organisation committee of Tournoi français des jeunes mathématiciennes et mathématiciens (TFJM) in Bordeaux[2]. A. Enge was a jury member.

R. Barbulescu takes part in the action for central Africa of the NGO Animath[3]. In 2022, an agreement was found with Université Virtuelle du Sénégal to organise the Alkindi contest in Senegal.

[1] URL Alkindi
[2] URL TJFM Bordeaux
[3] URL Animath

10.3.2 Articles and contents

R. Barbulescu published an article in the science section of “The conversation”, which was read by over 5000 people. The article is not adapted for the general public and quotes many research articles.[4]

R. Barbulescu published an article for the general public in the online version of the “Sud-Ouest” newspaper.[5]

10.3.3 Interventions

A. Enge took part in a discussion with middle school pupils around challenges in the digital world organised by Cap Sciences, INRIA and the Conseil National du Numérique.

X. Caruso was the corresponding researcher for an *atelier MATh.en.JEANS* for families in Cestas. Besides, he gave a talk at the final conference.

D. Robert gave a talk on *Les enjeux de la blockchain écologique* at the French tech days in Bordeaux, and at Unité a talk with E. Jeannot on *Les Cryptomonnaies et les NFT*.

A. Pellet-Mary facilitated two activities on cryptography for high school and middle school female students, during the week “Moi informaticienne moi mathématicienne”.

R. Barbulescu facilitated a workshop for highschool and IUT students about Cryptography for the Circuit scientifique at IMB.

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.

[4] URL The Conversation

[5] URL Sud-Ouest

[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.

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* 91 (2022), pp. 1405–1436. DOI: 10.1090/mcom/3697. URL: https://hal.science/hal-01822144.

[12] J.-F. Biasse, C. Fieker, T. Hofmann and A. Page. 'Norm relations and computational problems in number fields'. In: *Journal of the London Mathematical Society* (2022). DOI: 10.1112/jlms.12563. URL: https://hal.inria.fr/hal-02497890.

[13] X. Caruso. 'Where are the zeroes of a random p-adic polynomial?' In: *Forum of Mathematics, Sigma* 10 (July 2022), e55. DOI: 10.1017/fms.2022.27. URL: https://hal.science/hal-02557280.

[14] X. Caruso, A. David and A. Mézard. 'Can we dream of a 1-adic Langlands correspondence?' In: *Lecture Notes in Mathematics* (2023). URL: https://hal.science/hal-03648316.

[15] X. Caruso and A. Durand. 'Duals of linearized Reed-Solomon codes'. In: *Designs, Codes and Cryptography* 91.1 (2023), pp. 241–271. DOI: 10.1007/s10623-022-01102-7. URL: https://hal.science/hal-03395402.

[16] G. Castagnos, D. Catalano, F. Laguillaumie, F. Savasta and I. Tucker. 'Bandwidth-efficient threshold EC-DSA revisited: Online/Offline Extensions, Identifiable Aborts Proactive and Adaptive Security'. In: *Theoretical Computer Science* 939 (2023), pp. 78–104. DOI: 10.1016/j.tcs.2022.10.016. URL: https://hal.science/hal-03927198.

[17] G. Castagnos, F. Laguillaumie and I. Tucker. 'A tighter proof for CCA secure inner product functional encryption: Genericity meets efficiency'. In: *Theoretical Computer Science* 914 (May 2022), pp. 84–113. DOI: 10.1016/j.tcs.2022.02.014. URL: https://hal.inria.fr/hal-03780500.

[18] J. Kieffer. 'Degree and height estimates for modular equations on PEL Shimura varieties'. In: *Journal of the London Mathematical Society* 105.2 (11th Mar. 2022), pp. 1314–1361. DOI: 10.1112/jlms.12540. URL: https://hal.science/hal-02436057.

[19] J. Kieffer. 'Sign choices in the AGM for genus two theta constants'. In: *Publications Mathématiques de Besançon : Algèbre et Théorie des Nombres* (18th Aug. 2022), pp. 37–58. DOI: 10.5802/pmb.45. URL: https://hal.science/hal-02967220.

[20] J. Kieffer. 'Upper bounds on the heights of polynomials and rational fractions from their values'. In: *Acta Arithmetica* 203.1 (21st Mar. 2022), pp. 49–68. DOI: 10.4064/aa210816-26-1. URL: https://hal.science/hal-03226568.

[21] T. Kleinjung and B. Wesolowski. 'Discrete logarithms in quasi-polynomial time in finite fields of fixed characteristic'. In: *Journal of the American Mathematical Society* 35 (2022), pp. 581–624. DOI: 10.1090/jams/985. URL: https://hal.science/hal-03347994.

International peer-reviewed conferences

[22] K. Boudgoust, E. Gachon and A. Pellet-Mary. 'Some Easy Instances of Ideal-SVP and Implications on the Partial Vandermonde Knapsack Problem'. In: CRYPTO 2022. Vol. 13508. Santa Barbara / Hybrid, United States, 13th Aug. 2022. DOI: 10.1007/978-3-031-15979-4_17. URL: https://hal.science/hal-03789519.

[23] X. Caruso, T. Vaccon and T. Verron. 'On Polynomial Ideals And Overconvergence In Tate Algebras'. In: International Symposium On Symbolic And Algebraic Computation. Lille, France: ACM, 4th July 2022. DOI: 10.1145/3476446.3535491. URL: https://hal.science/hal-03574662.

[24] G. Castagnos, F. Laguillaumie and I. Tucker. 'Threshold Linearly Homomorphic Encryption on $\mathbf{Z}/2^k\mathbf{Z}$'. In: *Advances in Cryptology – ASIACRYPT 2022*. ASIACRYPT 2022 - International Conference on the Theory and Application of Cryptology and Information Security. Vol. 13792. Lecture Notes in Computer Science. Taipei, Taiwan: Springer Nature Switzerland, 2022, pp. 99–129. DOI: 10.1007/978-3-031-22966-4_4. URL: https://hal.science/hal-03936038.

[25] W. Castryck, M. Houben, F. Vercauteren and B. Wesolowski. 'On the decisional Diffie-Hellman problem for class group actions on oriented elliptic curves'. In: Fifteenth Algorithmic Number Theory Symposium, ANTS-XV. Fifteenth Algorithmic Number Theory Symposium, ANTS-XV. Bristol, United Kingdom, 8th Aug. 2022. URL: https://hal.science/hal-03805601.

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

[27] D. Lubicz and D. Robert. 'Fast change of level and applications to isogenies'. In: *Research in Number Theory*. ANTS 2022 - Fifteenth Algorithmic Number Theory Symposium. Vol. 9. 1. Bristol, United Kingdom, 2023, article n°7. DOI: 10.1007/s40993-022-00407-9. URL: https://hal.inria.fr/hal-03738315.

[28] P. Molin and A. Page. 'Computing groups of Hecke characters'. In: ANTS-XV 2022 - Fifteenth Algorithmic Number Theory Symposium. Bristol, United Kingdom, 13th Oct. 2022. URL: https://hal.inria.fr/hal-03795267.

[29] B. Wesolowski. 'Orientations and the supersingular endomorphism ring problem'. In: *Advances in Cryptology – EUROCRYPT 2022*. Advances in Cryptology – Eurocrypt 2022. Vol. 13277. Lecture Notes in Computer Science. Trondheim, Norway: Springer International Publishing, 25th May 2022, pp. 345–371. DOI: 10.1007/978-3-031-07082-2_13. URL: https://hal.science/hal-03799393.

[30] 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.science/hal-03340899.

Doctoral dissertations and habilitation theses

[31] J. Asuncion. 'Complex multiplication constructions of abelian extensions of quartic fields'. Université de Bordeaux; Universiteit Leiden (Leyde, Pays-Bas), 24th May 2022. URL: https://theses.hal.science/tel-03708516.

Reports & preprints

[32] R. Barbulescu and F. Jouve. *ECM And The Elliott-Halberstam Conjecture For Quadratic Fields*. Jan. 2023. URL: https://hal.science/hal-03485435.

[33] C. Bouvier, G. Castagnos, L. Imbert and F. Laguillaumie. *I want to ride my BICYCL: BICYCL Implements CryptographY in CLass groups*. 2022. URL: https://hal-lirmm.ccsd.cnrs.fr/lirmm-03863678.

[34] H. Cohen. *Elementary Continued Fractions for Linear Combinations of Zeta and L Values*. 2nd Dec. 2022. URL: https://hal.inria.fr/hal-03935509.

[35] J.-M. Couveignes and T. Ezome. *The equivariant complexity of multiplication in finite field extensions*. 11th Jan. 2023. URL: https://hal.science/hal-03410146.

[36] F. Johansson. *Computing elementary functions using multi-prime argument reduction*. 5th July 2022. URL: https://hal.inria.fr/hal-03714660.

[37] A. Maiga and D. Robert. *Towards computing canonical lifts of ordinary elliptic curves in medium characteristic*. 16th Mar. 2022. URL: https://hal.science/hal-03702658.

[38] D. Robert. *Breaking SIDH in polynomial time*. Aug. 2022. URL: https://hal.science/hal-03943959.

[39] D. Robert. *Evaluating isogenies in polylogarithmic time.* Aug. 2022. URL: https://hal.science/hal-03943970.

[40] D. Robert and A. Maiga. *Computing the Canonical Lift of Genus 2 Curves in Odd Characteristics.* 25th July 2022. URL: https://hal.science/hal-03738314.

[41] B. Wesolowski. *Computing isogenies between finite Drinfeld modules.* 4th June 2022. URL: https://hal.science/hal-03941045.

[42] A.-E. Wilke. *Convexity, plurisubharmonicity and the strong maximum modulus principle in Banach spaces.* 24th Oct. 2022. URL: https://hal.science/hal-03826538.

11.3 Other

Softwares

[43] [SW] C. Bouvier, G. Castagnos, L. Imbert and F. Laguillaumie, *BICYCL*, 2022. LIC: GNU General Public License v3.0 or later. HAL: ⟨lirmm-03827193⟩, URL: https://hal-lirmm.ccsd.cnrs.fr/lirmm-03827193, VCS: https://gite.lirmm.fr/crypto/bicycl, SWHID: ⟨swh:1:dir:b0fc22af0acbb995711313e71dda1a9b907e9e72;origin=https://hal.archives-ouvertes.fr/lirmm-03827193;visit=swh:1:snp:32a44231094baaaf2db6f7303a5712c6bc7c78d4;anchor=swh:1:rel:7ed7e725bcc693394b27e20adf146aad5bbd41c8;path=/⟩.

[44] [SW] A.-E. Wilke, *quartic* version 1.0, 22nd Nov. 2022. LIC: GNU General Public License v3.0 or later. HAL: ⟨hal-03879661⟩, URL: https://hal.science/hal-03879661, SWHID: ⟨swh:1:dir:3a34a6518fb3edb726bea0bf5b62fbbda58f83df;origin=https://hal.archives-ouvertes.fr/hal-03879661;visit=swh:1:snp:f4c274becc5c47cbe226d5d89be51d64506f2df0;anchor=swh:1:rel:5cb9f4297a94e6beefea69434353f62e25ad8480;path=/⟩.

11.4 Cited publications

[45] 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.

[46] 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.

[47] 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/.

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

[49] 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.

[50] 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/.

[51] 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/.