IN PARTNERSHIP WITH:
CNRS

Université de Bordeaux

Activity Report 2018

Project-Team LFANT

Lithe and fast algorithmic number theory

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

RESEARCH CENTER
Bordeaux - Sud-Ouest

THEME
Algorithmics, Computer Algebra and Cryptology

Table of contents

Project-Team LFANT

Creation of the Team: 2009 March 01, updated into Project-Team: 2010 January 01

Keywords:

Computer Science and Digital Science:

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, Visitors, External Collaborators

Research Scientists

Xavier Caruso [CNRS, Senior Researcher, from Oct 2018, HDR]
Andreas Enge [Team leader, Inria, Senior Researcher, HDR]
Fredrik Johansson [Inria, Researcher]
Aurel Page [Inria, Researcher]
Damien Robert [Inria, Researcher]

Faculty Members

Karim Belabas [Univ de Bordeaux, Professor, HDR]
Guilhem Castagnos [Univ de Bordeaux, Associate Professor]
Jean-Paul Cerri [Univ de Bordeaux, Associate Professor]
Henri Cohen [Univ de Bordeaux, Emeritus, until Aug 2018]
Jean-Marc Couveignes [Univ de Bordeaux, Professor, HDR]

PhD Students

Jared Guissmo Asuncion [Univ de Bordeaux]
Jean Kieffer [Ecole Normale Supérieure Paris, from Sep 2018]
Chloe Martindale [Universities Leiden and Bordeaux]
Emmanouil Tzortzakis [Universities Leiden and Bordeaux]
Abdoulaye Maiga [Univ. Dakar and Bordeaux]
Ida Tucker [ENS de Lyon and Bordeaux]

Technical staff

Bill Allombert [CNRS, from Sep 2018]

Administrative Assistants

Sabrina Blondel-Duthil [Inria]
Anne-Laure Gautier [Inria]

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, 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 $n \geqslant 3$. For recent textbooks, see [7]. 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 [38] 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, $\zeta_K(s) := \prod_{\mathfrak{p} \text{ prime ideal of } \mathcal{O}_K} \left(1 - \mathrm{N}\,\mathfrak{p}^{-s}\right)^{-1}$, 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: Karim Belabas, Guilhem Castagnos, Jean-Marc Couveignes, Andreas Enge, Damien Robert, Emmanouil Tzortzakis, 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 $\mathcal{C}(X, Y) = 0$ 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 $\mathcal{C} = Y^2 - (X^3 + aX + b)$ and *hyperelliptic curves* of equation $\mathcal{C} = Y^2 - (X^{2g+1} + \cdots)$ with $g \geqslant 2$.

The cryptosystem is implemented in an associated finite abelian group, the *Jacobian* $\mathrm{Jac}_{\mathcal{C}}$. 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 $\mathcal{C}$ is $K_{\mathcal{C}} = \mathbb{F}_q(X)[Y]/(\mathcal{C})$; it contains the *coordinate ring* $\mathcal{O}_{\mathcal{C}} = \mathbb{F}_q[X, Y]/(\mathcal{C})$. Definitions and properties carry over from the number field case $K/\mathbb{Q}$ to the function field extension $K_{\mathcal{C}}/\mathbb{F}_q(X)$. The Jacobian $\mathrm{Jac}_{\mathcal{C}}$ is the divisor class group of $K_{\mathcal{C}}$, which is an extension of (and for the curves used in cryptography usually equals) the ideal class group of $\mathcal{O}_{\mathcal{C}}$.

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 $(\sqrt{q}-1)^{2g} \leqslant |\operatorname{Jac}_{\mathcal{C}}| \leqslant (\sqrt{q}+1)^{2g}$, or $|\operatorname{Jac}_{\mathcal{C}}| \approx q^g$, 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 $\frac{\deg_X \mathcal{C}-1}{2}$. 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 $\operatorname{Jac}_{\mathcal{C}}$, it must be difficult to determine x. Computing x corresponds in fact to computing $\operatorname{Jac}_{\mathcal{C}}$ 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 $\mathcal{C}$ is a function that takes as input two elements of order n of $\operatorname{Jac}_{\mathcal{C}}$ 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, Chloe Martindale, Damien Robert.

Complex multiplication provides a link between number fields and algebraic curves; for a concise introduction in the elliptic curve case, see [41], for more background material, [40]. In fact, for most curves $\mathcal{C}$ over a finite field, the endomorphism ring of $\operatorname{Jac}_{\mathcal{C}}$, 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 $\mathcal{C}$ 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. Highlights of the Year

4.1. Highlights of the Year

Chloe Martindale defended her PhD thesis on *Isogeny Graphs, Modular Polynomials, and Applications*.

Antonin Riffaut defended his PhD thesis on *Effective computation of special points*.

A new release of PARI/GP, 2.11.0, has been published. This is a major stable release ending a development cycle which started in November 2016; it includes among others an extensive new package for modular forms.

2018 was also a year with more workshops on PARI/GP than ever: Besides two general workshops uniting developers and users, organised together with the universities of Besançon and Rome in the respective cities, the team participated with lectures on PARI/GP at the École jeunes chercheurs en théorie des nombres à Besançon (https://indico.math.cnrs.fr/event/2735/) and at the summer school ZETAS 2018 at Le Bourget du Lac (https://etzetas2018.sciencesconf.org/).

5. New Software and Platforms

5.1. APIP

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.

- Participant: Jérôme Milan
- Contact: Andreas Enge
- URL: http://www.lix.polytechnique.fr/~milanj/apip/apip.xhtml

5.2. AVIsogenies

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.

- Participants: Damien Robert, Gaëtan Bisson and Romain Cosset
- Contact: Damien Robert
- URL: http://avisogenies.gforge.inria.fr/

5.3. 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 FUNCTIONAL DESCRIPTION: Features - Precisions beyond 300000 bits are now supported by an addition chain of variable length for the -function. Dependencies - The minimal version number of Mpfr has been increased to 3.0.0, that of Mpc to 1.0.0 and that of Pari to 2.7.0.

- Participant: Andreas Enge
- Contact: Andreas Enge
- URL: http://www.multiprecision.org/cm/home.html

5.4. CMH

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.

- Participants: Andreas Enge, Emmanuel Thomé and Regis Dupont
- Contact: Emmanuel Thomé
- URL: http://cmh.gforge.inria.fr

5.5. 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.

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

5.6. Euclid

KEYWORD: Number theory
FUNCTIONAL DESCRIPTION: Euclid is a program to compute the Euclidean minimum of a number field. It is the practical implementation of the algorithm described in [38] . Some corresponding tables built with the algorithm are also available. Euclid is a stand-alone program depending on the PARI library.

- Participants: Jean-Paul Cerri and Pierre Lezowski
- Contact: Jean-Paul Cerri
- URL: http://www.math.u-bordeaux1.fr/~plezowsk/euclid/index.php

5.7. KleinianGroups

KEYWORDS: Computational geometry - Computational number theory
FUNCTIONAL DESCRIPTION: KleinianGroups is a Magma package that computes fundamental domains of arithmetic Kleinian groups.

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

5.8. 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 FUNCTIONAL DESCRIPTION: Fixed `mp\_pow`, see http://lists.gforge.inria.fr/pipermail/mpc-discuss/2014-October/001315.html - `\#18257`: Switched to libtool 2.4.5.

- Participants: Andreas Enge, Mickaël Gastineau, Paul Zimmermann and Philippe Théveny
- Contact: Andreas Enge
- URL: http://www.multiprecision.org/

5.9. 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 FUNCTIONAL DESCRIPTION: - new function `produc\_an\_hecke` - improved memory consumption for unbalanced FFT multiplications

- Participant: Andreas Enge
- Contact: Andreas Enge
- URL: http://www.multiprecision.org/mpfrcx/home.html

5.10. 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.

- Participants: Andreas Enge, Hamish Ivey-Law, Henri Cohen and Karim Belabas
- Partner: CNRS
- Contact: Karim Belabas
- URL: http://pari.math.u-bordeaux.fr/

6. New Results

6.1. Cryptographic Protocols

Participants: Guilhem Castagnos, Ida Tucker.

In [24], G. Castagnos, F. Laguillaumie and I. Tucker revisit a recent cryptographic primitive called *Functional encryption for inner products* (FE4IP).

Functional encryption (FE) is an advanced cryptographic primitive which allows, for a single encrypted message, to finely control how much information on the encrypted data each receiver can recover. To this end many functional secret keys are derived from a master secret key. Each functional secret key allows, for a ciphertext encrypted under the associated public key, to recover a specific function of the underlying plaintext.

Since constructions for general FE that appear in the past five years are far from practical, the problem arose of building efficient FE schemes for restricted classes of functions; and in particular for linear functions, (i.e. the inner product functionality). Such constructions yield many practical applications, while developing our understanding of FE.

Though such schemes had already been conceived in the past three years (Abdalla *et al.* 2015, Agrawal *et al.* 2016), they all suffered of practical drawbacks. Namely the computation of inner products modulo a prime are restricted, in that they require that the resulting inner product be small for decryption to be efficient. The only existing scheme that overcame this constraint suffered of poor efficiency due in part to very large ciphertexts. This work overcomes these limitations and we build the first FE schemes for inner products modulo a prime that are both efficient and recover the result whatever its size.

To this end, Castagnos *et al.* introduce two new cryptographic assumptions. These are variants of the assumptions used for the Castagnos-Laguillaumie encryption of 2015. This supposes the existence of a cyclic group G where the decision Diffie-Hellman assumption holds together with a subgroup F of G where the discrete logarithm problem is easy. This setting allows to encode information in the exponent of the subgroup F, which can be efficiently recovered whatever its size.

From these assumptions Castagnos *et al.* construct generic, linearly homomorphic encryption schemes over a field of prime order which are semantically secure under chosen plaintext attacks. They then use the homomorphic properties of the above schemes to construct generic inner product FE schemes over the integers and over fields of prime order. They thereby provide constructions for inner product FE modulo a prime p that do not restrict the size of the inputs or of the resulting inner product, which are the most efficient such schemes to date.

This paper was presented at the ASIACRYPT Conference 2018, and is part of the ALAMBIC project.

6.2. Computation of Euclidean minima in totally definite quaternion fields

Participant: Jean-Paul Cerri.

In collaboration with Pierre Lezowski, Jean-Paul Cerri has studied norm-Euclidean properties of totally definite quaternion fields over number fields. Building on their previous work about number fields, they have proved that the Euclidean minimum and the inhomogeneous minimum of orders in such quaternion fields are always equal. Besides, they are rational under the hypothesis that the base number field is not quadratic. This single remaning open case corresponds to the similar open case remaining for real number fields.

They also have extended Cerri's algorithm for the computation of the upper part of the norm-Euclidean spectrum of a number field to this noncommutative context. This algorithm has allowed to compute the exact value of the norm-Euclidean minimum of orders in totally definite quaternion fields over a quadratic number field. This has provided the first known values of this minimum when the base number field has degree strictly greater than 1.

Consequently, both theoretical and practical milestones set in the previous quadrennial report were reached. These results are presented in [19], due to appear in *International Journal of Number Theory*.

6.3. Can you hear the homology of 3-dimensional drums?

Participant: Aurel Page.

In [16], A. Bartel and A. Page describe all possible actions of groups of automorphisms on the homology of 3-manifolds, and prove that for every prime p, there are 3-dimensional drums that sound the same but have different p-torsion in their homology. This completes previous work [42] by proving that the behaviour observed by computer experimentation was indeed a general phenomenon.

More precisely: if M is a manifold with an action of a group G, then the homology group $H_1(M,\mathbb{Q})$ is naturally a $\mathbb{Q}[G]$-module, where $\mathbb{Q}[G]$ denotes the rational group ring. Bartel and Page prove that for every finite group G, and for every $\mathbb{Q}[G]$-module V, there exists a closed hyperbolic 3-manifold M with a free G-action such that the $\mathbb{Q}[G]$-module $H_1(M,\mathbb{Q})$ is isomorphic to V. They give an application to spectral geometry: for every finite set P of prime numbers, there exist hyperbolic 3-manifolds N and N' that are strongly isospectral such that for all $p \in P$, the p-power torsion subgroups of $H_1(N,\mathbb{Z})$ and of $H_1(N',\mathbb{Z})$ have different orders. They also show that, in a certain precise sense, the rational homology of oriented Riemannian 3-manifolds with a G-action "knows" nothing about the fixed point structure under G, in contrast to the 2-dimensional case. The main geometric techniques are Dehn surgery and, for the spectral application, the Cheeger-Müller formula, but they also make use of tools from different branches of algebra, most notably of regulator constants, a representation theoretic tool that was originally developed in the context of elliptic curves.

6.4. Error-correcting codes based on non-commutative algebras

Participant: Aurel Page.

In [36], C. Maire and A. Page revisit a construction due to Lenstra and Guruswami by generalising them 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 division algebras of any degree, and estimate the smallest possible size of the alphabet in terms of the degree of the algebra.

6.5. Towards practical key exchange from ordinary isogeny graphs

Participant: Jean Kieffer.

In [25], L. De Feo, J. Kieffer and B. Smith revisit the ordinary isogeny-graph based cryptosystems of Couveignes and Rostovtsev–Stolbunov, long dismissed as impractical.

De Feo, Kieffer and Smith give algorithmic improvements that accelerate key exchange in this framework, and explore the problem of generating suitable system parameters for contemporary pre-and post-quantum security that take advantage of these new algorithms. They prove the session-key security of this key exchange in the Canetti-Krawczyk model, and the IND-CPA security of the related public-key encryption scheme, under reasonable assumptions on the hardness of computing isogeny walks. This system admits efficient key-validation techniques that yield CCA-secure encryption, thus providing an important step towards efficient post-quantum non-interactive key exchange (NIKE).

6.6. Optimal addition sequences for theta functions

Participants: Andreas Enge, Fredrik Johansson.

In [20], A. Enge, F. Johansson and their coauthor W. Hart consider the problem of numerically evaluating one-dimensional θ-functions and the elliptic η-function. They construct short addition sequences reaching an optimal number of $N + o(N)$ multiplications for evaluating the function as a sparse series with N terms. The proof relies on the representability of specific quadratic progressions of integers as sums of smaller numbers of the same kind. For example, they show that every generalised pentagonal number $c > 5$ can be written as $c = 2a + b$, where a, b are smaller generalised pentagonal numbers. They then give a baby-step giant-step algorithm that breaks through the theoretical barrier achievable with addition sequences, and which uses only $O(N/(logN)^r)$ multiplications for any $r > 0$. These theoretical improvements also lead to an interesting speed-up in practice, and they have been integrated into the CM and the ARB software.

6.7. Reed–Solomon-Gabidulin Codes

Participant: Xavier Caruso.

In [31], X. Caruso and A. Durand define a new family of linear codes which is a common generalization of Reed–Solomon codes on the one hand and Gabidulin codes on the other hand. Their construction works over an arbitrary field (not necessarily finite) equipped with an automorphism of finite order and a twisted derivation whose subfield of constants is sufficiently large. This setting allows for example the base field to be $\mathbb{F}_q(t)$ equipped with its natural derivation and then provides a new large family of interesting codes. Caruso and Durand then compute the minimal distance of their codes and design an efficient algorithm for decoding up to the half of the minimal distance.

6.8. Computing Stieltjes constants using complex integration

Participant: Fredrik Johansson.

In [32], F. Johansson and I. Blagouchine devise an efficient algorithm to compute the generalized Stieltjes constants $\gamma_n(a)$ to arbitrary precision with rigorous error bounds, for the first time achieving this with low complexity with respect to the order n. The algorithm consists of locating an approximate steepest descent contour and then evaluating the integral numerically in ball arithmetic using the Petras algorithm with a Taylor expansion for bounds near the saddle point. An implementation is provided in the Arb library.

6.9. Numerical Evaluation of Elliptic Functions, Elliptic Integrals and Modular Forms

Participant: Fredrik Johansson.

In [33], F. Johansson describes algorithms to compute elliptic functions and their relatives (Jacobi theta functions, modular forms, elliptic integrals, and the arithmetic-geometric mean) numerically to arbitrary precision with rigorous error bounds for arbitrary complex variables. Implementations in ball arithmetic are available in the Arb library. This overview article discusses the standard algorithms from a concrete implementation point of view, and also presents some improvements.

6.10. Numerical integration in arbitrary-precision ball arithmetic

Participant: Fredrik Johansson.

In [26], F. Johansson describes an implementation of arbitrary-precision numerical integration with rigorous error bounds in the Arb library. Rapid convergence is ensured for piecewise complex analytic integrals by use of the Petras algorithm, which combines adaptive bisection with adaptive Gaussian quadrature where error bounds are determined via complex magnitudes without evaluating derivatives. The code is general, easy to use, and efficient, often outperforming existing non-rigorous software.

6.11. Fast and rigorous arbitrary-precision computation of Gauss-Legendre quadrature nodes and weights

Participant: Fredrik Johansson.

In [26], F. Johansson and M. Mezzarobba describe a strategy for rigorous arbitrary-precision evaluation of Legendre polynomials on the unit interval and its application in the generation of Gauss-Legendre quadrature rules. The focus is on making the evaluation practical for a wide range of realistic parameters, corresponding to the requirements of numerical integration to an accuracy of about 100 to 100 000 bits. The algorithm combines the summation by rectangular splitting of several types of expansions in terms of hypergeometric series with a fixed-point implementation of Bonnet's three-term recurrence relation. Rigorous enclosures of the Gauss-Legendre nodes and weights are then computed using the interval Newton method. The work provides rigorous error bounds for all steps of the algorithm. The approach is validated by an implementation in the Arb library, which achieves order-of-magnitude speedups over previous code for computing Gauss-Legendre rules with simultaneous high degree and precision.

6.12. On a two-valued sequence and related continued fractions in power series fields

Participant: Bill Allombert.

In [15], Bill Allombert with Nicolas Brisebarre and Alain Lasjaunias describe a noteworthy transcendental continued fraction in the field of power series over $\mathbb{Q}$, having irrationality measure equal to 3. This article has been published in The Ramanujan Journal.

6.13. Moduli space

Participant: Nicolas Mascot.

The article [22] by Nicolas Mascot, on the Certification of modular Galois representations has been published in Mathematics of Computation.

6.14. Modular forms

Participants: Karim Belabas, Henri Cohen, Bill Allombert.

In [18], K. Belabas and H. Cohen give theoretical and practical information on the Pari/GP modular forms package, using the formalism of trace formulas. This huge package (about 70 exported public functions) handles standard operations on classical modular forms in $M_k(\Gamma_0(N), \chi)$, also in weight 1 and non-integral weight (which are not cohomological, hence not directly handled by trace formulas). It is the first publicly available package which can compute Fourier expansions at any cusps, evaluate modular forms near the real axis, evaluate L-functions of non-eigenforms, and compute general Petersson scalar products.

In [39], H. Cohen explained how to compute Fourier expansions at all cusps of any modular form of integral or half-integral weight.

A complementary package using modular symbols is used in [17] by Karim Belabas, Dominique Bernardi and Bernadette Perrin-Riou to compute Manin's constant and the modular degree of elliptic curves defined over $\mathbb{Q}$.

6.15. L-functions

Participant: Henri Cohen.

In [29], H. Cohen gives an overview of Computational Number Theory in Relation with L-Functions, both in the local case (counting points on varieties over finite fields, involving in particular a detailed study of Gauss and Jacobi sums), and in the global case (for instance Dirichlet L-functions, involving in particular the study of inverse Mellin transforms). He also gives a number of little-known but very useful numerical methods, usually but not always related to the computation of L-functions.

6.16. Number fields

Participant: Henri Cohen.

In https://hal.inria.fr/hal-01379473/, H. Cohen and F. Thorne give explicit formulas for the Dirichlet series generating function of D_ℓ-extensions of odd prime degree ℓ with given quadratic resolvent.

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR Alambic – AppLicAtions of MalleaBIlity in Cryptography

Participant: Guilhem Castagnos.

https://crypto.di.ens.fr/projects:alambic:main

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 realized that, in specific settings, malleability in cryptographic protocols can actually be a very useful feature. For example, the notion of homomorphic encryption allows specific types of computations to be carried out on ciphertexts and 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 for fully homomorphic encryption enables widespread use of cloud computing by ensuring the confidentiality of processed data.

The aim of the ALAMBIC project 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.

7.1.2. ANR CLap–CLap – The p-adic Langlands correspondence: a constructive and algorithmical approach

Participant: Xavier Caruso.

The p-adic Langlands correspondence has become nowadays one of the deepest and the most stimulating research programs in number theory. It was initiated in France in the early 2000's by Breuil and aims at understanding the relationships 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 organize.

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 shall 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 will also be the opportunity to contribute to the development of the mathematical software SAGEMATH and to the expansion of computational methodologies.

7.2. European Initiatives

7.2.1. H2020 Projects

Title: OpenDreamKit

Program: H2020

Duration: January 2016 - December 2020

Coordinator: Nicolas Thiéry

Inria contact: Karim Belabas

Description http://cordis.europa.eu/project/rcn/198334_en.html, http://opendreamkit.org

OpenDreamKit is a Horizon 2020 European Research Infrastructure project (#676541) that will run for four years, starting from September 2015. It provides substantial funding to the open source computational mathematics ecosystem, and in particular popular tools such as LinBox, MPIR, SageMath, GAP, Pari/GP, LMFDB, Singular, MathHub, and the IPython/Jupyter interactive computing environment.

7.3. International Initiatives

7.3.1. Inria International Labs

International Laboratory for Research in Computer Science and Applied Mathematics
Associate Team involved in the International Lab:

7.3.1.1. FAST

Title: (Harder Better) FAster STronger cryptography

International Partner

Université des Sciences et Techniques de Masuku (Gabon) - Tony Ezome and the PRMAIS project

Start year: 2017

See also: https://www.inria.fr/en/associate-team/fast

The project aims to develop better algorithms for elliptic curve cryptography with prospect of the two challenges ahead: - securing the internet of things - preparing towards quantum computers.

Elliptic curves are currently the fastest public-key cryptosystem (with a key size that can fit on embeded devices) while still through a different mode of operation beeing (possibly) able to resist quantum based computers.

Activities for this year involved:

- Tony Ezome organised a Cimpa school on Courbes algébriques pour une arithmétique efficace des corps finis from 17/11/2018 - 30/11/2018 in Ziguinchor (Sénégal), Institution Université Assane Seck de Ziguinchor.
- Abdoul Asiz Ciss and Damien Robert represented the team at the Journées du Lirima. One of the suggestion was to find industrial collaborations in Africa, especially in Senegal. Ongoing work is done by the team to find such a collaboration, especially on the new challenges of post-quantum cryptography.
- Abdoulaye Maiga visited in Bordeaux to work with Damien Robert from 22/10/2018 to 18/01/2019. Tony Ezome and Mohamadou Sall visited from 08/12/2018 to 22/12/2018.

Activities for this year involved the funding of Luca De Feo to speak at the EMA "Mathématiques pour la Cryptographie Post-quantique et Mathématiques pour le Traitement du Signal", organised by Djiby Sow and Abdoul Asiz Ciss organised an EMA at the École Polytechnique de Thiès (Sénégal) from May 10 to May 23, about "Cryptographie à base d'isogénies"; the visit of Abdoulaye Maiga to the LFANT team where he worked with Damien Robert to find absolute invariants of good reduction modulo 2 for abelian surfaces; and the organisation by Damien Robert of a workshop in Bordeaux with most of the team members from September 04 to September 08. The slides or proceedings are available at https://lfant.math.u-bordeaux.fr/index.php?category=seminar&page=2017.

7.3.2. *Inria International Partners*

7.3.2.1. Informal International Partners

The team is used to collaborate with Leiden University through the ALGANT program for PhD joint supervision.

Eduardo Friedman (U. of Chile), long term collaborator of K. Belabas and H. Cohen is a regular visitor in Bordeaux (about 1 month every year).

7.4. International Research Visitors

7.4.1. *Visits of International Scientists*

- Nicolas Mascot (American University of Beirut, Lebanon) visited the team for a week (8-12/01/2018).
- Alex Bartel (University of Glasgow, UK) visited the team for two weeks (27/03/2018 to 07/04/2018).
- Takashi Fukuda (Nihon University, Japan) visited the team for two months (20/01/2018 to 25/03/2018)
- Tony Ezome (Université des Sciences et Techniques de Masuku) and Mohamadou Sall (Dakar) visited the team for two weeks in December. Abdoul Aziz (Dakar) visited the team for one week in September.
- Abdoulaye Maiga visited the team for three months, from October to January 2019.

Researchers visiting the team to give a talk to the team seminar include Elie Eid (Université de Rennes), Jean-François Biasse (University of South Florida), Francesco Battistoni (University of Milan), Alex Bartel (Glasgow University), Tristan Vaccon (Université de Limoges), and Takashi Fukuda (Nihon University).

7.4.2. *Visits to International Teams*

A. Page visited Alex Bartel (University of Glasgow, UK) for two weeks (16-27/07/2018) and Michael Lipnowski (McGill University, Montreal, Canada) for two weeks (10-23/11/2018).

A. Page and Alex Bartel did a research stay in Oberwolfach (Allemagne) with the Research In Pairs programme for three weeks (14/10/2018-3/11/2018).

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. *Scientific Events Organisation*

8.1.1.1. Member of the Editorial Boards

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

X. Caruso is an editor and one of the founder of the journal *Annales Henri Lebesgue*.

H. Cohen is an editor for the Springer book series *Algorithms and Computations in Mathematics (ACM)*.

J.-M. Couveignes is a member of the editorial board (scientific committee) of the *Publications mathématiques de Besançon* since 2010.

From January 2015 to September 2018 J.-M. Couveignes was a member of the scientific council of the Fondation Mathématique de Paris.

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

8.1.2. Invited Talks

A. Page: *Algorithms for the cohomology of compact arithmetic manifolds and Hecke operators* in the Simons collaboration conference *Arithmetic Geometry, Number Theory, and Computation*, MIT (Boston, US), August 20-24, 2018.

8.1.3. Scientific Expertise

K. Belabas is a member of the 'conseil scientifique' of the Société Mathématique de France

8.1.4. Research Administration

Since January 2017, A. Enge is "délégué scientifique" of the Inria research centre Bordeaux–Sud-Ouest. As such, he is also a designated member of the "commission d'évaluation" of Inria.

Since January 2015, K. Belabas is vice-head of the Math 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.

He is an elected member of "commission de la recherche" in the academic senate of Bordeaux University.

He is a member of the "Conseil National des Université" (25th section, pure mathematics).

J.-P. Cerri is an elected member of the scientific council of the Mathematics Institute of Bordeaux (IMB) and responsible for the bachelor programme in mathematics and informatics.

From January 2015 until January 2019, J.-M. Couveignes was the head of the Math Institute (IMB). He is head of the Scientific Committee of the Albatros (ALliance Bordeaux universities And Thales Research in AviOnicS) long term cooperation between Inria, Bordeaux-INP, Université de Bordeaux and CNRS.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Master : G. Castagnos, *Cryptanalyse*, 60h, M2, University of Bordeaux, France;

Master : G. Castagnos, *Cryptologie avancée*, 30h, M2, University of Bordeaux, France;

Master : G. Castagnos, *Courbes elliptiques*, 60h, M2, University of Bordeaux, France;

Master : D. Robert, *Courbes elliptiques*, 60h, M2, University of Bordeaux, France;

Master : K. Belabas, *Computer Algebra*, 91h, M2, University of Bordeaux, France;

Master : J.-M. Couveignes, *Algorithmic Arithmetic*, 30h, M2, University of Bordeaux, France;

Master : J.-M. Couveignes, *Modules, espaces quadratiques*, 30h, M1, University of Bordeaux, France;

Licence : Jean-Paul Cerri, Algèbre linéaire 2, 51h TD, L2, Université de Bordeaux, France

Licence : Jean-Paul Cerri, Arithmétique et Cryptologie, 24h TD, L3, Université de Bordeaux, France

Licence : Jean-Paul Cerri, Structures algébriques 2, 35h TD, L3, Université de Bordeaux, France

Master : Jean-Paul Cerri, Cryptologie, 60h TD, M1, Université de Bordeaux, France

Master : Jean-Paul Cerri, 3 TER, Université de Bordeaux, France

Licence : Jean Kieffer, Mathématiques pour la biologie, 64h TD, L1, Université de Bordeaux, France

8.2.2. Supervision

PhD: Chloe Martindale, *Isogeny graphs, modular polynomials, and applications*, defended in 2018, supervised by A. Enge and Marco Streng (Universiteit Leiden).

PhD: Antonin Riffaut *Calcul effectif de points spéciaux*, defended in 2018, supervised by Y. Bilu and K. Belabas.

PhD in progress : Ida Tucker, *Design of new advanced cryptosystems from homomorphic building blocks*, since October 2017, supervised by Guilhem Castagnos and Fabien Laguillaumie

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 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: Emmanouil Tzortzakis *Algorithms for $\mathbb{Q}$-curves*, supervised by K. Belabas, P. Bruin and B. Edixhoven.

PhD in progress: Pavel Solomatin *Topics on L-functions*, supervised by B. de Smit and K. Belabas.

PhD in progress: Jean Kieffer *Isogénies et endomorphismes de variétés abéliennes*, supervised by D. Robert and A. Page.

Master thesis: Amandine Malonguemfo Teagho *Algorithms for isometries of lattices*, supervised by A. Page.

Master thesis: William Dallaporta *Bhargava's theory and parametrization of algebraic structures*, supervised by K. Belabas.

8.2.3. Juries

X. Caruso has written a report for the doctoral dissertation by Robin Bartlett, King's College in London: *On the reductions of some crystalline representations*.

A. Enge has written a report for the doctoral dissertation by Benjamin Wesolowski, École polytechnique fédérale de Lausanne: *Arithmetic & Geometric Structures in Cryptography*.

A. Enge has written a report for the professorial dissertation by Luca De Feo, Université de Versailles–Saint Quentin: *Exploring Isogeny Graphs*.

8.3. Popularization

8.3.1. Articles and contents

- X. Caruso published an article entitled *Polynômes tordus* in the journal *Au fil des maths de la maternelle à l'université...* edited by APMEP.
- H. Cohen wrote in [28] an introduction to Modular forms, which has been published in the book Notes from the International School on Computational Number Theory.

8.3.2. Education

D. Robert is a member of the jury of Agregations de Mathematiques. He is also the codirector with Alain Couvreur of the option “calcul formel” of the Modelisation part of the oral examination.

8.3.3. Interventions

- 24/02/2018 in Olot (Spain), A. Page, with the other participants of Sage Days 93: one day for 20 local high school students to explore mathematical problems.
- 24/05/2018, A. Page: Unithé ou café on the mathematics of wireless communications: *Méthodes algébriques et géométriques pour les communications sans fil : comment l'espace hyperbolique peut-il améliorer vos appels téléphoniques ?*
- 30/05/2018, A. Page: in Poitiers half a day meeting with junior school students who took part in the Al-Kindi competition; introduction to cryptography.
- 27/09/2018 D. Robert and A. Page: demonstration stand on graph-based cryptography at the Inria BSO Party Day.
- 9-11/10/201 A. Page: Fête de la Science at Inria Bordeaux, activity on cryptography (7 groups of students).
- 13/10/2018 D. Robert and A. Page: demonstration stand on graph-based cryptography at the Inria BSO Open Day.
- 11/12/2018 A. Page: talk at the Inria BSO Comité des Projets *Variations arithmétiques et algorithmiques sur le thème << Peut-on entendre la forme d'un tambour? >>*

9. Bibliography

Major publications by the team in recent years

[1] E. Bayer-Fluckiger, J.-P. Cerri, J. Chaubert. *Euclidean minima and central division algebras*, in "International Journal of Number Theory", 2009, vol. 5, n^{o} 7, pp. 1155–1168, http://www.worldscinet.com/ijnt/05/0507/S1793042109002614.html

[2] K. Belabas, M. Bhargava, C. Pomerance. *Error estimates for the Davenport-Heilbronn theorems*, in "Duke Mathematical Journal", 2010, vol. 153, n^{o} 1, pp. 173–210, http://projecteuclid.org/euclid.dmj/1272480934

[3] J. Belding, R. Bröker, A. Enge, K. Lauter. *Computing Hilbert class polynomials*, in "Algorithmic Number Theory — ANTS-VIII", Berlin, A. van der Poorten, A. Stein (editors), Lecture Notes in Computer Science, Springer-Verlag, 2007, vol. 5011, http://hal.inria.fr/inria-00246115

[4] X. Caruso, J. L. Borgne. *A new faster algorithm for factoring skew polynomials over finite fields*, in "J. Symbolic Comput.", 2018, vol. 79, pp. 411–443

[5] X. Caruso, D. Roe, T. Vaccon. *Tracking p-adic precision*, in "LMS J. Comput. Math.", 2014, vol. 17, pp. 274–294

[6] J.-P. Cerri. *Euclidean minima of totally real number fields: algorithmic determination*, in "Math. Comp.", 2007, vol. 76, n^{o} 259, pp. 1547–1575, http://www.ams.org/journals/mcom/2007-76-259/S0025-5718-07-01932-1/

[7] H. Cohen. *Number Theory I: Tools and Diophantine Equations; II: Analytic and Modern Tool*, Graduate Texts in Mathematics, Springer-Verlag, New York, 2007, vol. 239/240

[8] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, F. Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Discrete mathematics and its applications, Chapman & Hall, Boca Raton, 2006

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

[10] A. Enge. *The complexity of class polynomial computation via floating point approximations*, in "Mathematics of Computation", 2009, vol. 78, n^{o} 266, pp. 1089–1107, http://www.ams.org/mcom/2009-78-266/S0025-5718-08-02200-X/home.html

[11] A. Enge, P. Gaudry, E. Thomé. *An L(1/3) Discrete Logarithm Algorithm for Low Degree Curves*, in "Journal of Cryptology", 2011, vol. 24, n^{o} 1, pp. 24–41

[12] D. Lubicz, D. Robert. *Computing isogenies between abelian varieties*, in "Compositio Mathematica", 09 2012, vol. 148, n^{o} 05, pp. 1483–1515, http://dx.doi.org/10.1112/S0010437X12000243

Publications of the year

Doctoral Dissertations and Habilitation Theses

[13] C. Martindale. *Isogeny graphs, modular polynomials, and applications*, Université de Bordeaux, June 2018, https://tel.archives-ouvertes.fr/tel-01992715

[14] A. Riffaut. *Effective computation of special points*, Université de Bordeaux, July 2018, https://tel.archives-ouvertes.fr/tel-01931307

Articles in International Peer-Reviewed Journals

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

[16] A. Bartel, A. Page. *Group representations in the homology of 3-manifolds*, in "Commentarii Mathematici Helvetici", 2019, https://arxiv.org/abs/1605.04866 , https://hal.inria.fr/hal-01671748

[17] K. Belabas, D. Bernardi, B. Perrin-Riou. *La constante de Manin et le degré modulaire d'une courbe elliptique*, in "Publications Mathématiques de Besançon : Algèbre et Théorie des Nombres", 2019, https://hal.archives-ouvertes.fr/hal-01766202

[18] K. Belabas, H. Cohen. *Modular Forms in Pari/GP*, in "Research in the Mathematical Sciences ", 2018, https://arxiv.org/abs/1810.00547 , https://hal.inria.fr/hal-01883565

[19] J.-P. Cerri, P. Lezowski. *Computation of Euclidean minima in totally definite quaternion fields*, in "International Journal of Number Theory", 2018, 19 pages, some minor corrections; to appear, https://hal.archives-ouvertes.fr/hal-01447059

[20] A. Enge, W. Hart, F. Johansson. *Short addition sequences for theta functions*, in "Journal of Integer Sequences", 2018, vol. 18, n^{o} 2, pp. 1-34, https://arxiv.org/abs/1608.06810 , https://hal.inria.fr/hal-01355926

[21] F. JOHANSSON, M. MEZZAROBBA. *Fast and rigorous arbitrary-precision computation of Gauss-Legendre quadrature nodes and weights*, in "SIAM Journal on Scientific Computing", 2018, vol. 40, n^{o} 6, pp. C726-C747, https://arxiv.org/abs/1802.03948 [*DOI :* 10.1137/18M1170133], https://hal.inria.fr/hal-01705612

[22] N. MASCOT. *Certification of modular Galois representations*, in "Mathematics of Computation", 2018, vol. 87, n^{o} 309, pp. 381–423, https://arxiv.org/abs/1312.6418 , https://hal.archives-ouvertes.fr/hal-01426832

[23] A. RIFFAUT. *Equations with powers of singular moduli*, in "International Journal of Number Theory", 2019, To appear in International Journal of Number Theory, https://hal.archives-ouvertes.fr/hal-01630363

International Conferences with Proceedings

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

[25] L. DE FEO, J. KIEFFER, B. SMITH. *Towards practical key exchange from ordinary isogeny graphs*, in "ASIACRYPT 2018", Brisbane, Australia, December 2018, https://arxiv.org/abs/1809.07543 , https://hal.inria.fr/hal-01872817

[26] F. JOHANSSON. *Numerical integration in arbitrary-precision ball arithmetic*, in "Mathematical Software – ICMS 2018", Notre Dame, United States, Lecture Notes in Computer Science, Springer, 2018, n^{o} 10931, pp. 255–263, https://hal.inria.fr/hal-01714969

Scientific Books (or Scientific Book chapters)

[27] X. CARUSO. *Computations with p-adic numbers*, in "Journées Nationales de Calcul Formel", Les cours du CIRM, 2018, https://arxiv.org/abs/1701.06794 , https://hal.archives-ouvertes.fr/hal-01444183

[28] H. COHEN. *An Introduction to Modular Forms*, in "Notes from the International School on Computational Number Theory;Izmir Institute of Technology 2017", E. BÜYÜKAIK, I. INAM (editors), Springer Birkhäuser, 2018, https://arxiv.org/abs/1809.10907 , https://hal.inria.fr/hal-01883058

[29] H. COHEN. *Computational Number Theory in Relation with L-Functions*, in "Notes from the International School on Computational Number Theory; Izmir Institute of Technology 2017", E. BÜYÜKAIK, I. INAM (editors), Springer Birkhäuser, 2018, https://arxiv.org/abs/1809.10904 , https://hal.inria.fr/hal-01883052

Other Publications

[30] X. CARUSO. *Polynômes de Ore en une variable*, January 2018, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01673910

[31] X. CARUSO, A. DURAND. *Reed-Solomon-Gabidulin Codes*, December 2018, https://arxiv.org/abs/1812.09147 - working paper or preprint, https://hal.archives-ouvertes.fr/hal-01949409

[32] F. JOHANSSON, I. V. BLAGOUCHINE. *Computing Stieltjes constants using complex integration*, 2018, https://arxiv.org/abs/1804.01679 - working paper or preprint, https://hal.inria.fr/hal-01758620

[33] F. Johansson. *Numerical Evaluation of Elliptic Functions, Elliptic Integrals and Modular Forms*, June 2018, https://arxiv.org/abs/1806.06725 - working paper or preprint, https://hal.inria.fr/hal-01817952

[34] F. Johansson. *Faster arbitrary-precision dot product and matrix multiplication*, January 2019, https://arxiv.org/abs/1901.04289 - working paper or preprint, https://hal.inria.fr/hal-01980399

[35] E. Lorenzo García, P. Kiliçer, M. Streng. *Primes dividing invariants of CM Picard curves*, January 2018, https://arxiv.org/abs/1801.04682 - working paper or preprint, https://hal.archives-ouvertes.fr/hal-01685037

[36] C. Maire, A. Page. *Codes from unit groups of division algebras over number fields*, 2018, https://arxiv.org/abs/1804.07108 - working paper or preprint, https://hal.inria.fr/hal-01770396

[37] C. Martindale. *Hilbert Modular Polynomials*, January 2019, working paper or preprint, https://hal.inria.fr/hal-01990298

References in notes

[38] K. Belabas. *L'algorithmique de la théorie algébrique des nombres*, in "Théorie algorithmique des nombres et équations diophantiennes", N. Berline, A. Plagne, C. Sabbah (editors), 2005, pp. 85–155

[39] H. Cohen. *Expansions at Cusps and Petersson Products in Pari/GP*, in "Elliptic Integrals, Functions, and Modular Forms in Quantum Field Theory", Zeuthen, Germany, Elliptic Integrals, Functions, and Modular Forms in Quantum Field Theory, Springer Wien, October 2017, https://hal.inria.fr/hal-01883070

[40] H. Cohen, P. Stevenhagen. *Computational class field theory*, in "Algorithmic Number Theory — Lattices, Number Fields, Curves and Cryptography", J. Buhler, P. Stevenhagen (editors), MSRI Publications, Cambridge University Press, 2008, vol. 44

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

[42] A. Page, A. Bartel. *Torsion homology and regulators of isospectral manifolds*, in "Journal of topology", December 2016, vol. 9, n^{o} 4, pp. 1237 - 1256 [*DOI :* 10.1112/jtopol/jtw023], https://hal.inria.fr/hal-01671812