IN PARTNERSHIP WITH:
CNRS

Université de Bordeaux

Activity Report 2014

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

Keywords: Algorithmic Number Theory, Complexity, Computer Algebra, Cryptology, High Performance Computing

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

1. Members

Research Scientists

Andreas Enge [Team leader, Inria, Senior Researcher, HdR]
Damien Robert [Inria, Researcher]

Faculty Members

Karim Belabas [Univ. Bordeaux I, Professor, HdR]
Guilhem Castagnos [Univ. Bordeaux I, Associate Professor, until Aug 2014]
Jean-Paul Cerri [Univ. Bordeaux I, Associate Professor]
Henri Cohen [Univ. Bordeaux I, HdR]
Jean-Marc Couveignes [Univ. Bordeaux I, Professor, HdR]

Engineers

Bill Allombert [CNRS]
Hamish Ivey-Law [Inria, granted by FP7 ERC ANTICS STG project]

PhD Students

Athanasios Angelakis [Universities Leiden and Bordeaux]
Julio Brau Avila [Universities Leiden and Bordeaux]
Iuliana Ciocanea Teodorescu [Universities Leiden and Bordeaux]
Pınar Kılıçer [Universities Leiden and Bordeaux]
Chloë Martindale [Universities Leiden and Bordeaux]
Nicolas Mascot [Univ. Bordeaux, until Aug 2014]
Enea Milio [Inria, FP7 ERC ANTICS STG project]
Aurel Page [Univ. Bordeaux, until Aug 2014]

Post-Doctoral Fellows

Barinder Banwait [Inria, until Dec 2014, granted by FP7 ERC ANTICS STG project]
Sorina Ionica [Univ. Bordeaux, from Jul 2014]
Fredrik Johansson [Inria, from Sep 2014]
Pierre Lezowski [Inria, granted by FP7 ERC ANTICS STG project]

Administrative Assistants

Anne-Laure Gautier [Inria]
Flavie Tregan [Inria, from May 2014 until Sep 2014]

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, Athanasios Angelakis, Karim Belabas, Julio Brau Avila, Jean-Paul Cerri, Henri Cohen, Jean-Marc Couveignes, Andreas Enge, Pınar Kılıçer, Pierre Lezowski, Nicolas Mascot, 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 [5]. 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 [35] 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, Julio Brau Avila, Jean-Marc Couveignes, Andreas Enge, Hamish Ivey-Law, Nicolas Mascot, Enea Milio, Damien Robert.

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: Karim Belabas, Henri Cohen, Jean-Marc Couveignes, Andreas Enge, Hamish Ivey-Law, Chloë Martindale, Nicolas Mascot, Enea Milio, Aurel Page, Damien Robert.

Complex multiplication provides a link between number fields and algebraic curves; for a concise introduction in the elliptic curve case, see [37], for more background material, [36]. 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* $\operatorname{Gal}_{H/K}$ 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 $\operatorname{Gal}_{H/K}$ 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. New Software and Platforms

4.1. Pari/Gp

Participants: Karim Belabas [correspondent], Bill Allombert, Henri Cohen, Andreas Enge, Hamish Ivey-Law.

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

PARI/GP is a widely used computer algebra system designed for fast computations in number theory (factorisation, algebraic number theory, elliptic curves, ...), 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.

- PARI is a C library, allowing fast computations.
- GP is an easy-to-use interactive shell giving access to the PARI functions.
- gp2c, the GP-to-C compiler, combines the best of both worlds by compiling GP scripts to the C language and transparently loading the resulting functions into GP; scripts compiled by gp2c will typically run three to four times faster.
- Version of PARI/GP: 2.7.2
- Version of gp2c: 0.0.9
- License: GPL v2+
- Programming language: C

4.2. GNU MPC

Participants: Andreas Enge [correspondent], Mickaël Gastineau [CNRS], Philippe Théveny [INRIA project-team ARIC], Paul Zimmermann [INRIA project-team CARAMEL].

http://mpc.multiprecision.org/.

GNUMPC 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 GNU MPFR.

It is a prerequisite for the GNU compiler collection GCC since version 4.5, where it is used in the C and Fortran front ends for constant folding, the evaluation of constant mathematical expressions during the compilation of a program. Since 2011, it is an official GNU project.

2012 has seen the first release of the major version 1.0.

- Version: 1.0.2 *Fagus silvatica*
- License: LGPL v3+
- ACM: G.1.0 (Multiple precision arithmetic)
- AMS: 30.04 Explicit machine computation and programs
- APP: Dépôt APP le 2003-02-05 sous le numéro IDDN FR 001 060029 000 R P 2003 000 10000
- Programming language: C

4.3. MPFRCX

Participant: Andreas Enge.

http://mpfrcx.multiprecision.org/

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.

- Version: 0.4.2 *Cassava*
- License: LGPL v2.1+
- Programming language: C

4.4. CM

Participant: Andreas Enge.

http://cm.multiprecision.org/

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. For the implemented algorithms, see [8].

- Version: 0.2 *Blindhühnchen*
- License: GPL v2+
- Programming language: C

4.5. AVIsogenies

Participants: Damien Robert [correspondent], Gaëtan Bisson, Romain Cosset [INRIA project-team CARAMEL].

http://avisogenies.gforge.inria.fr/.

AVISOGENIES (Abelian Varieties and Isogenies) 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.

- Version: 0.6
- License: LGPL v2.1+
- Programming language: Magma

4.6. APIP

Participant: Jérôme Milan.

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

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.

- Version: 2012-10-17
- License: GPL v2+
- Programming language: C with libpari

4.7. CMH

Participants: Andreas Enge, Emmanuel Thomé [INRIA project-team CARAMEL].

http://cmh.gforge.inria.fr/

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

- Version: 1.0
- License: GPL v3+
- Programming language: C

4.8. Cubic

Participant: Karim Belabas.

http://www.math.u-bordeaux1.fr/~belabas/research/software/cubic-1.2.tgz

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.

- Version: 1.2
- License: GPL v2+
- Programming language: C

4.9. Euclid

Participant: Pierre Lezowski.

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

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.

- Version: 1.2
- License: LGPL v2+
- Programming language: C

4.10. KleinianGroups

Participant: Aurel Page.

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

KLEINIANGROUPS is a Magma package that computes fundamental domains of arithmetic Kleinian groups.

- Version: 1.0
- License: GPL v3+
- Programming language: Magma

5. New Results

5.1. Highlights of the Year

Aurel Page has defended his PhD thesis on *Méthodes explicites pour les groupes arithmétiques* [12] in July 2014. Nicolas Mascot has defended his PhD thesis on *Computing modular Galois representations* [11], in July 2014.

5.2. Class groups and other invariants of number fields

Participants: Karim Belabas, Jean-Paul Cerri, Pierre Lezowski.

In [21], P. Lezowski describes the explicit computation of the Euclidean minimum of a number field. It has been published in Mathematics of Computation.

Ohno and Nakagawa have proved, relations between the counting functions of certain cubic fields. These relations may be viewed as complements to the Scholz reflection principle, and Ohno and Nakagawa deduced them as consequences of 'extra functional equations' involving the Shintani zeta functions associated to the prehomogeneous vector space of binary cubic forms. In [26], Henri Cohen, Simon Rubinstein-Salzedo and Frank Thorne generalize their result by proving a similar identity relating certain degree fields with Galois groups D and F respectively, for any odd prime, and in particular we give another proof of the Ohno–Nakagawa relation without appealing to binary cubic forms.

The article [16] by H. Cohen and F. Thorne, H. Cohen on Dirichlet series associated to cubic fields with given resolvent has been published. This article gives an explicit formula for the Dirichlet series $\sum_K |\Delta(K)|^{-s}$, where the sum is over isomorphism classes of all cubic fields whose quadratic resolvent field is isomorphic to a fixed quadratic field k.

This work is extended in [15] where H. Cohen give efficient numerical methods for counting exactly the number of D_ℓ number fields of degree ℓ with given quadratic resolvent, for calculating the constants occurring in their asymptotic expansions, and give tables for typical cases.

5.3. Number and function fields

Participants: Jean-Marc Couveignes, Karim Belabas.

In the article [29], J. Brau study the growth of the Galois invariants of the p-Selmer group of an elliptic curve in a degree p Galois extension. He shows that this growth is determined by certain local cohomology groups and determine necessary and sufficient conditions for these groups to be trivial.

In the article [30] written with J. Nathan, J. Brau study the modular curve $X'(6)$ of level 6 defined over $\mathbb{Q}$ whose $\mathbb{Q}$-rational points correspond to j-invariants of elliptic curves E over $\mathbb{Q}$ for which $\mathbb{Q}(E[2])$ is a subfield of $\mathbb{Q}(E[3])$. They characterize the j-invariants of elliptic curves with this property by exhibiting an explicit model of $X'(6)$. $X'(6)(\mathbb{Q})$ gives an infinite family of examples of elliptic curves with non-abelian "entanglement fields," which is relevant to the systematic study of correction factors of various conjectural constants for elliptic curves over $\mathbb{Q}$.

5.4. Quaternion algebras

Participants: Jean-Paul Cerri, Pierre Lezowski, Aurel Page.

In the article [14] written with J. Chaubert, J.-P. Cerri and P. Lezowski study totally indefinite Euclidean quaternion fields over a number field K, that is to say where no infinite place is ramified. Relying on some generalisation of Hasse–Schilling–Maaß Norm Theorem, they prove that the Euclidean property of K implies the Euclidean property of any totally indefinite Euclidean quaternion field over K. Conversely, they provide the complete list of norm-Euclidean and totally indefinite quaternion fields over an imaginary quadratic number field. In particular, the article exhibits a totally indefinite and norm-Euclidean quaternion field over a non-Euclidean number field. This provides an answer to a question by Eichler. The proofs are both theoretic and algorithmic. The article has been published in Acta Arithmetica.

Deciding whether an ideal of a number field is principal and finding a generator is a fundamental problem with many applications in computational number theory. In the article [25] gives a an algorithm for indefinite quaternion algebras by reducing the decision problem to that in the underlying number field. It also gives an heuristically subexponential algorithm for finding a generator.

5.5. Complex multiplication and modularity

Participants: Jean-Marc Couveignes, Andreas Enge, Nicolas Mascot, Enea Milio, Aurel Page, Damien Robert.

A. Enge and E. Thomé describe in [20] a quasi-linear algorithm for computing Igusa class polynomials of Jacobians of genus 2 curves via complex floating-point approximations of their roots. After providing an explicit treatment of the computations in quartic CM fields and their Galois closures, they pursue an approach due to Dupont for evaluating θ-constants in quasi-linear time using Newton iterations on the Borchardt mean. They report on experiments with the implementation CMH and present an example with class number 20016.

In [34] E. Milio explains how to generalise the work of Régis Dupont for computing modular polynomials in dimension 2 to invariants derived from theta constants. Modular polynomials have many applications. In particular, they could speed up the CRT-algorithm to compute class fields of degree 4 CM-fields which would lead to faster algorithms to construct cryptographically secure Jacobians of hyperelliptic curves. They are also used to compute graphs of isogenies. This paper presents how to compute modular polynomials and the polynomials computed and then it proves some of their properties.

With F. Morain, A. Enge has determined exhaustively under which conditions "generalised Weber functions", that is, simple quotients of η functions of not necessarily prime transformation level and not necessarily of genus 1, yield class invariants [19]. The result is a new infinite family of generators for ring class fields, usable to determine complex multiplication curves. They examine in detail which lower powers of the functions are applicable, thus saving a factor of up to 12 in the size of the class polynomials, and describe the cases in which the polynomials have integral rational instead of integral quadratic coefficients.

N. Mascot has continued his work on computing Galois representations attached to Jacobians of modular curves. He has given tables of modular Galois representations in [33] obtained using the algorithm of [39]. He has computed Galois representations modulo primes up to 31 for the first time. In particular, he has computed the representations attached to a newform with non-rational (but of course algebraic) coefficients, which had never been done before. These computations take place in the Jacobians of modular curves of genus up to 26.

5.6. Elliptic curve and Abelian varieties cryptology

Participants: Jean-Marc Couveignes, Andreas Enge, Damien Robert.

In [27] J.-M. Couveignes and T. Ezome show how to efficiently evaluate functions, including Weil functions and canonical Theta functions, on Jacobian varieties and their quotients. They deduce a quasi-optimal algorithm to compute (l, l) isogenies between Jacobians of genus two curves, using a compact representation and differential characterisation of isogenies in this context. This work has been submitted to the LMS Journal of Computation and Mathematics.

The paper [18] by J.-M. Couveignes and R. Lercier describing the problem of parameterisations by radicals of low genus algebraic curves has been accepted in *Advances in mathematics of communications*.

In [31] D. Lubicz and D. Robert explain how to improve the arithmetic of Abelian and Kummer varieties. The speed of the arithmetic is a crucial factor in the performance of abelian varieties based cryptosystem. Depending on the cryptographic application, the speed record holder are elliptic curves (in the Edwards model) or the Kummer surface of an hyperelliptic curves of genus 2 (in the level 2 theta model). One drawback of the Kummer surface is that only scalar multiplications are available, which may be a drawback in certain cryptographic protocols. The previous known models to work on the Jacobian rather than the Kummer surface (Mumford coordinates or theta model of level 4) are too slow and not competitive with Elliptic Curves. This paper explains how to use geometric properties (like projective normality) to speed up the arithmetic. In particular it introduces a novel addition algorithm on Kummer varieties (compatible additions), and use it to enhance multi-exponentiations in Kummer varieties and to obtain new models of abelian surfaces where the scalar multiplication is as fast as on the Kummer surface.

In [32] (which has been accepted at LMS Journal of Computation and Mathematics), D. Lubicz and D. Robert explain how to compute isogenies between abelian varieties given algebraic equation of the kernel. The previous algorithms to compute isogenies between abelian varieties needed the coordinates of generators of the kernel. One drawback was that even if the kernel is rational, these generators may live in extension of large degree, especially for Abelian varieties defined over a number field rather than a finite field. This paper combines the use of formal coordinates together with a normalisation alongs linear subspaces of the kernel rather than the whole kernel to derive an algorithm which is quasi-optimal if the degree of the isogeny is ℓ^g, for ℓ congruent to 1 modulo 4.

This article expands the article [17] by D. Cosset and D. Robert about the computation of (ℓ, ℓ)-isogenies in dimension 2 which has been published in Mathematics of Computation.

5.7. Pairings

Participants: Andreas Enge, Damien Robert.

The article [22] by D. Lubicz and D. Robert explaining how to compute optimal pairings on abelian varieties described by their theta models has been accepted for publication at Journal of Symbolic Computation.

In [24], A. Enge and J. Milan report on the APIP implementation of cryptographic pairings on elliptic curves in PARI/GP. For security levels equivalent to the different AES flavours, they exhibit suitable curves in parametric families and show that optimal ate and twisted ate pairings exist and can be efficiently evaluated. They provide a correct description of Miller's algorithm for signed binary expansions such as the NAF and extend a recent variant due to Boxall et al. to addition-subtraction chains. They analyse and compare several algorithms proposed in the literature for the final exponentiation. Finally, they give recommendations on which curve and pairing to choose at each security level.

6. Partnerships and Cooperations

6.1. National Initiatives

6.1.1. ANRPeace – Parameter spaces for Efficient Arithmetic and Curve security Evaluation

Participants: Bill Allombert, Karim Belabas, Jean-Marc Couveignes, Andreas Enge, Hamish Ivey-Law, Nicolas Mascot, Enea Milio, Aurel Page, Damien Robert.

http://chic2.gforge.inria.fr/

The PEACE project is joint between the research teams of Institut de Recherche en Mathématiques de Rennes (IRMAR), LFANT and Institut Mathématiques de Luminy (IML).

The project aims at constituting a comprehensive and coherent approach towards a better understanding of theoretical and algorithmic aspects of the discrete logarithm problem on algebraic curves of small genus. On the theoretical side, this includes an effective description of moduli spaces of curves and of abelian varieties, the maps that link these spaces and the objects they classify. The effective manipulation of moduli objects will allow us to develop a better understanding of the algorithmic difficulty of the discrete logarithm problem on curves, which may have dramatic consequences on the security and efficiency of already deployed cryptographic devices.

One of the anticipated outcomes of this proposal is a new set of general criteria for selecting and validating cryptographically secure curves (or families of curves) suitable for use in cryptography. Instead of publishing fixed curves, as is done in most standards, we aim at proposing generating rationales along with explicit theoretical and algorithmic criteria for their validation.

The ANR organised the conference “Effective moduli spaces and applications to cryptography” in June 2014 as a part of the Centre Henri Lebesgue’s Thematic Semester 2014 “Around moduli spaces”.

6.1.2. ANRSimpatic – SIM and PAiring Theory for Information and Communications security

Participants: Guilhem Castagnos, Damien Robert.

The SIMPATIC project is an industrial research project, formed by academic research teams and industrial partners: Orange Labs, École Normale Supérieure, INVIA, Oberthur Technologies, ST-Ericsson France, Université de Bordeaux 1, Université de Caen Basse-Normandie, Université de Paris 8.

The aim of the SIMPATIC project is to provide the most efficient and secure hardware/software implementation of a bilinear pairing in a SIM card. This implementation will then be used to improve and develop new cryptographic algorithms and protocols in the context of mobile phones and SIM cards. The project will more precisely focus on e-ticketing and e-cash, on cloud storage and on the security of contactless and of remote payment systems.

D. Robert is a participant in the Task 2 whose role is to give state of the art algorithms for pairing computations, adapted to the specific hardware requirements of the Simpatic Project.

6.2. European Initiatives

6.2.1. FP7 & H2020 Projects

6.2.1.1. ANTICS

Type: FP7

Defi: NC

Instrument: ERC Starting Grant

Objectif: NC

Duration: January 2012 - December 2016

Coordinator: Inria (France)

Inria contact: Andreas Enge

Abstract: Data security and privacy protection are major challenges in the digital world. Cryptology contributes to solutions, and one of the goals of ANTICS (Algorithmic Number Theory in Cryptology) is to develop the next generation public key cryptosystem, based on algebraic curves and abelian varieties. Challenges to be tackled are the complexity of computations, certification of the computed results and parallelisation, addressed by introducing more informatics into algorithmic number theory.

6.3. International Initiatives

6.3.1. Inria International Labs

The *MACISA* project-team (Mathematics Applied to Cryptology and Information Security in Africa) is one of the new teams of LIRIMA. Researchers from Inria and the universities of Bamenda, Bordeaux, Dakar, Franceville, Maroua, Ngaoundéré, Rennes, Yaoundé cooperate in this team.

The project is concerned with public key cryptology and more specifically the role played by algebraic maps in this context. The team focus on two themes:

- Theme 1 : Rings, primality, factoring and discrete logarithms;
- Theme 2 : Elliptic and hyperelliptic curve cryptography.

The project is managed by a team of five permanent researchers: G. Nkiet, J.-M. Couveignes, T. Ezome, D. Robert and A. Enge. Since Sep. 2014 the coordinator is T. Ezome and the vice-coordinator is D. Robert. The managing team organises the cooperation, schedules meetings, prepares reports, controls expenses, reports to the LIRIMA managing team and administrative staff.

A non-exhaustive list of activities organised or sponsored by Macisa includes

- The Summer school in M'Bour in Senegal with the International Center for Pure and Applied Mathematics (ICPAM/CIMPA), June 2014;
- The Annual Cameroonian workshop on Cryptography, Algebra and Geometry (CRAG), July 2014;
- The visit of Thierry Mefenza (Cameroun), to École Normale Supérieure de Paris for a PhD Thesis with Damien Vergnault, November 2013 and September–November 2014;
- The visit of Hortense Boudjou (Maroua) to work with Abdoul Aziz Ciss (École Polytechnique de Thièse, Sénégal), May – July 2014;
- The visit of Abdoul Aziz Ciss (Dakar) and Tony Ezome (Franceville) to Bordeaux, September 2014.
- Kodjo Kpognon Egadédé defended his PhD thesis in december 2014 under the supervision of Julien Sebag.

The team was evaluated in September 2014 as part of the general LIRIMA evaluation seminar.

6.3.2. Inria International Partners

6.3.2.1. 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).

6.4. International Research Visitors

6.4.1. Visits of International Scientists

- Hartmut Monien, Universität Bonn, Germany. 01/2014;
- Eduardo Friedman, Universidad de Chile, 02/2014;
- Amalia Pizarro-Madariaga, Universidad de Valparaiso, Chile, 04/2014;
- Tony Ezome Mintsa, University of Franceville, Gabon, 04/2014 and 09/2014;
- Alina Dudeanu, École polytechnique fédérale de Lausanne, Switzerland, 05/2014;
- Kamal Khuri-Makdisi, American University of Beirut, Lebanon, 07/2014;
- Abdoul-Aziz Ciss, University of Dakar, 09/2014;
- Dimitar Jetchev, École polytechnique fédérale de Lausanne, Switzerland, 10/2014;

6.4.1.1. Internships

- Ilaria Chillotti (with D. Robert), Université Joseph Fourier, 02/2014–07/2014]
- Gregor Seiler (with A. Enge), Technische Universität Berlin, Germany, 10/2013–03/2014

7. Dissemination

7.1. Promoting Scientific Activities

7.1.1. Scientific events organisation

7.1.1.1. member of the organizing committee

The team helped organising the Colloque Jeunes Chercheurs en Théorie des Nombres, which took place in Bordeaux on 11/06/2014–13/06/2014.

7.1.2. Scientific events selection

7.1.2.1. member of the conference program committee

Andreas Enge was a member of the programme committee for the *Elliptic Curve Cryptography* 2014 conference in Chennai, India.

Sorina Ionica was a member of the program committee for the *Latincrypt* 2014 conference.

7.1.3. Journal

7.1.3.1. member of the editorial board

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

H. Cohen is an editorial board member of *Journal de Théorie des Nombres de Bordeaux*; he is an editor for the Springer book series *Algorithms and Computations in Mathematics (ACM).*

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

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

7.1.4. Other scientific activities

7.1.4.1. Invited talks

- D. Robert was invited to give a talk on “Pairings on abelian varieties and the Discrete Logarithm Problem” for the Discrete Logarithm Problem Conference in May 2014 at Ascona, Switzerland
- D. Robert was invited to give a talk on “Isogenies between abelian varieties” for the Effective moduli spaces and applications to cryptography conference in June 2014 at Rennes
- D. Robert was invited to give a talk on “Optimal pairings on abelian varieties” for the Elliptic Curve Cryptography conference in October 2014 at Chennai, India
- H. Ivey-Law was invited to give a talk on “Arithmetic on Jacobians of Relative Curves” for the Number Theory Meets Geometry conference in November 2014 at Kaiserslautern, Germany
- A. Enge has given an invited talk on “Abelian varieties and theta functions for cryptography” at the 4th International Cryptology and Information Security Conference at Putrajaya, Malaysia
- A. Enge has given an invited talk on “Class invariants for Abelian surfaces” at the workshop Computational Number Theory of Foundations of Computational Mathematics in Montevideo, Uruguay

7.1.4.2. Seminar

The following external speakers have given a presentation at the LFANT seminar, see
http://lfant.math.u-bordeaux1.fr/index.php?category=seminar

- Frédérique Oggier (NTU, Singapour): “ Le codage pour le stockage distribué de données”
- Hartmut Monien (Physikalisches Institut der Universität Bonn): “Zeta values, random matrix theory and Euler-MacLaurin summation” and “Calculating rational coverings for subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ efficiently”
- Nicolas Delfosse (Montreal): “Une introduction au calcul quantique tolérant aux fautes”
- Eduardo Friedman (Universidad de Chile): “Cône de Shintani et degré topologique”
- John Boxall (Caen): “Heuristiques sur les variétés abéliennes adaptées à la cryptographie à couplage”
- Pınar Kılıçer (Leiden+IMB): “The class number one problem for genus-2 curves”
- Bertrand Maury (Paris-Sud): “Arbre bronchique infini et entiers dyadiques”

- Emmanuel Thomé (Nancy): “Un algorithme quasi-polynomial de calcul de logarithme discret en petite caractéristique”
- Oriol Serra (UPC, Barcelone): “Algebraic Removal Lemma ”
- Amalia Pizarro-Madariaga (Valparaíso): “Estimations for the Artin conductor”
- Alina Dudeanu (EPFL): “Computing a Velu type formula for rational cyclic isogenies betweeniso-morphism classes of Jacobians of genus two curves that are defined over afinite field.”
- Gaetan Bisson (University of French Polynesia): “On polarised class groups of orders in quartic CM-fields”
- Kamal Khuri Makdisi (American University of Beirut): “Moduli interpretation of Eisenstein series”
- Kamal Khuri Makdisi (American University of Beirut): “On divisor group arithmetic for typical divisors on curves”
- Chloe Martindale (University of Leiden / IMB): “An algorithm for computing Hilbert modular varieties”
- Dimitar Jetchev (EPFL): “Euler systems from special cycles on unitary Shimura varieties andarith-metic applications”
- Alain Couvreur (Inria and LIX, École Polytechnique): “Une attaque polynomiale du schéma de McEliece basé sur les codes de Goppa "sauvages".”

7.1.4.3. Research administration

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 research” in the academic senate of Bordeaux University.

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.

Since January 2011, J.-M. Couveignes is involved in the *GDR mathématiques et entreprises* and in the *Agence pour les mathématiques en interaction avec l'entreprise et la société*.

A. Enge is the head of the COST-GTRI, the Inria body responsible for the scientific evaluation of the international partnerships of the institute.

7.2. Teaching - Supervision - Juries

7.2.1. Teaching

Summer school: A. Enge, Complex multiplication of elliptic curves and Pairings on elliptic curves, 6h, Putrajaya, Malaysia

Master: K. Belabas, Computer Algebra, 90h, M2, Université de Bordeaux

Master: K. Belabas, Computational number theory, 50h, M2, Université de Bordeaux

Master: K. Belabas, Number theory, 24h, M1, Université de Bordeaux

Licence: K. Belabas, C2i, 24h, L1, Université de Bordeaux

Licence: Jean-Paul Cerri, Codes et cryptologie, 34.67h, TD niveau L1, Université de Bordeaux

Licence: Jean-Paul Cerri, Algèbre 4, 50.67h, TD niveau L3, Université de Bordeaux

Licence: Jean-Paul Cerri, Cryptographie et Arithmétique, 24h, Cours niveau L3, Université de Bordeaux

Master, Jean-Paul Cerri, Arithmétique, 36h, Cours niveau M1, Université de Bordeaux

Encadrement, Jean-Paul Cerri, Encadrement d'un projet tuteuré (L3) et d'un TER (M1), Université de Bordeaux

Master: J.-M. Couveignes, Algorithms for public key cryptography, 40h, M2, Université Bordeaux, France;

Master: J.-M. Couveignes, Algorithms for number fields, 40h, M2, Université Bordeaux, France;

Licence : E. Milio, Topologie et Fonctions de plusieurs variables, 36 heures, niveau L2, université de Bordeaux site Victoire, France

Master: Sorina Ionica, Encadrement de 3 projets master (M2 CSI), Un iversité de Bordeaux.

7.2.2. Supervision

PhD: Aurel Page, *Méthodes explicites pour les groupes arithmétiques*, [12], supervised by K. Belabas and A. Enge, defended 07/2014

PhD: Nicolas Mascot, *Computing modular Galois representations* [11], supervised by K. Belabas and J.-M. Couveignes, defended 07/2014

PhD in progress: Enea Milio, *Isogénies entre surfaces abéliennes*, University Bordeaux, supervised by A. Enge and D. Robert

PhD in progress: Pınar Kılıçer, *Topics in complex multiplication*, Universities Bordeaux and Leiden, supervised by A. Enge and M. Streng

PhD in progress: Chloë Martindale, *Isogeny graphs*, Universities Bordeaux and Leiden, supervised by A. Enge and M. Streng

7.2.3. Juries

D. Robert was a member of the committee for the PhD defense of Christophe Tran in Rennes (December 2013).

A. Enge was a referee for the PhD of Nicole Sutherland, University of Sydney, entitled “Algorithms for Galois extensions of Global Function Fields”.

7.3. Popularization

K. Belabas gave a lecture to present Bhargava’s works (2014 Fields medal) to high school teachers during the “Journée de l’IREM d’Aquitaine” (11/2014, about 100 attendants).

A. Enge has presented “Les maths au service du secret (et de sa découverte!)” during the Math en Jeans congress held in Bordeaux in April 2014, for an audience of highschool pupils aged 12 to 17.

He has spoken on “Mathematik für (und gegen!) das Geheimnis” in an event in July at Gymnasium Leopoldinum, Detmold, Germany, to an audience comprised of pupils aged 12 to 18 and of mathematics teachers.

At the GNU Hacker’s Meeting 2014 in München, Germany, he has presented a tutorial on “GnuPG key signing”.

8. 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] 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/

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

[6] 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 & HallBoca Raton, 2006

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

[8] 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

[9] 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

[10] 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

[11] N. MASCOT. *Computing modular Galois representations*, Universite de Bordeaux, July 2014, https://hal.archives-ouvertes.fr/tel-01110658

[12] A. PAGE. *Explicit methods for arithmetic groups*, Université de Bordeaux, July 2014, https://tel.archives-ouvertes.fr/tel-01111509

Articles in International Peer-Reviewed Journals

[13] K. BELABAS, E. FRIEDMAN. *Computing the residue of the Dedekind zeta function*, in "Mathematics of Computation", 2015, vol. 84, pp. 357-369, 16 pages, https://hal.inria.fr/hal-00916654

[14] J.-P. CERRI, J. CHAUBERT, P. LEZOWSKI. *Totally indefinite Euclidean quaternion fields*, in "Acta Arithmetica", 2014, vol. 165, n^{o} 2, pp. 181-200, https://hal.archives-ouvertes.fr/hal-01016614

[15] H. COHEN. *Exact counting of D_ℓ number fields with given quadratic resolvent*, in "Mathematics of Computation", 2014, forthcoming, https://hal.archives-ouvertes.fr/hal-01027417

[16] H. Cohen, F. Thorne. *Dirichlet series associated to cubic fields with given quadratic resolvent*, in "Michigan Mathematical Journal", 2014, vol. 63, pp. 253-273, https://hal.inria.fr/hal-00854662

[17] R. Cosset, D. Robert. *Computing (l,l)-isogenies in polynomial time on Jacobians of genus 2 curves*, in "Mathematics of Computation", November 2014, 23 p. , forthcoming [*DOI :* 10.1090/S0025-5718-2014-02899-8], https://hal.archives-ouvertes.fr/hal-00578991

[18] J.-M. Couveignes, R. Lercier. *The geometry of some parameterizations and encodings*, in "Advances in mathematics of communications", December 2014, vol. 8, n^{o} 4, 22 p. [*DOI :* 10.3934/amc.2014.8.437], https://hal.archives-ouvertes.fr/hal-00870112

[19] A. Enge, F. Morain. *Generalised Weber Functions*, in "Acta Arithmetica", 2014, vol. 164, n^{o} 4, pp. 309-341 [*DOI :* 10.4064/aa164-4-1], https://hal.inria.fr/inria-00385608

[20] A. Enge, E. Thomé. *Computing class polynomials for abelian surfaces*, in "Experimental Mathematics", 2014, vol. 23, pp. 129-145 [*DOI :* 10.1080/10586458.2013.878675], https://hal.inria.fr/hal-00823745

[21] P. Lezowski. *Computation of the Euclidean minimum of algebraic number fields*, in "Mathematics of Computation", 2014, vol. 83, pp. 1397-1426, 30 pages, shorter version, with many typos fixed [*DOI :* 10.1090/S0025-5718-2013-02746-9], https://hal.archives-ouvertes.fr/hal-00632997

[22] D. Lubicz, D. Robert. *A generalisation of Miller's algorithm and applications to pairing computations on abelian varieties*, in "Journal of Symbolic Computation", 2015, vol. 67, pp. 68-92 [*DOI :* 10.1016/j.jsc.2014.08.001], https://hal.inria.fr/hal-00806923

[23] A. Page. *Computing arithmetic Kleinian groups*, in "Mathematics of Computation", 2014, 29 p. , forthcoming, https://hal.archives-ouvertes.fr/hal-00703043

International Conferences with Proceedings

[24] A. Enge, J. Milan. *Implementing cryptographic pairings at standard security levels*, in "Security, Privacy, and Applied Cryptography Engineering", Pune, India, R. S. Chakraborty, V. Matyas, P. Schaumont (editors), Lecture Notes in Computer Science, Springer, October 2014, vol. 8804, pp. 28-46 [*DOI :* 10.1007/978-3-319-12060-7_3], https://hal.inria.fr/hal-01034213

[25] A. Page. *An algorithm for the principal ideal problem in indefinite quaternion algebras*, in "ANTS XI", GyeongJu, South Korea, August 2014, https://hal.archives-ouvertes.fr/hal-00996346

Other Publications

[26] H. Cohen, S. Rubinstein-Salzedo, F. Thorne. *Identitites for Field Extensions Generalizing the Ohno–Nakagawa Relations*, 2015, https://hal.inria.fr/hal-01109980

[27] J.-M. Couveignes, T. Ezome. *Computing functions on Jacobians and their quotients*, November 2014, https://hal.archives-ouvertes.fr/hal-01088933

[28] A. Enge. *Bilinear pairings on elliptic curves*, February 2014, https://hal.inria.fr/hal-00767404

[29] B. JULIO. *Selmer groups of elliptic curves in degree p extensions*, 2014, https://hal.archives-ouvertes.fr/hal-01111745

[30] B. JULIO, J. NATHAN. *Elliptic curves with 2-torsion contained in the 3-torsion field*, January 2015, https://hal.archives-ouvertes.fr/hal-01111744

[31] D. LUBICZ, D. ROBERT. *Arithmetic on Abelian and Kummer Varieties*, June 2014, https://hal.archives-ouvertes.fr/hal-01057467

[32] D. LUBICZ, D. ROBERT. *Computing separable isogenies in quasi-optimal time*, February 2014, Accepted for publication at LMS Journal of Computation and Mathematics, https://hal.archives-ouvertes.fr/hal-00954895

[33] N. MASCOT. *Tables of modular Galois representations*, 2014, https://hal.archives-ouvertes.fr/hal-01110252

[34] E. MILIO. *A quasi-linear algorithm for computing modular polynomials in dimension 2*, November 2014, https://hal.archives-ouvertes.fr/hal-01080462

References in notes

[35] 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

[36] 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

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

[38] P. LEZOWSKI. *Computation of the Euclidean minimum of algebraic number fields*, 2011, To appear in Mathematics of Computation, 30 pages, http://hal.archives-ouvertes.fr/hal-00632997

[39] N. MASCOT. *Computing modular Galois representations*, in "Rendiconti del Circolo Matematico di Palermo", December 2013, vol. 62, n^o 3, pp. 451-476 [*DOI :* 10.1007/S12215-013-0136-4], https://hal.archives-ouvertes.fr/hal-00776606