IN PARTNERSHIP WITH:
CNRS

Université de Bordeaux

Activity Report 2015

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:

4.3.1. - Public key cryptography
7.12. - Computer arithmetic
7.6. - Computer Algebra
7.7. - Number theory

Other Research Topics and Application Domains:

6. - IT and telecom
9.4.2. - Mathematics

1. Members

Research Scientists

Andreas Enge [Team leader, Inria, Senior Researcher, HdR]
Fredrik Johansson [Inria, Researcher]
Damien Robert [Inria, Researcher]
Enea Milio [Univ. Bordeaux]

Faculty Members

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

Engineers

Bill Allombert [CNRS]
Hamish Ivey-Law [Inria, until Nov 2015, granted by FP7 ERC ANTICS STG project]

PhD Students

Julio Brau Avila [Universities Leiden and Bordeaux, until Jun 2015]
Iuliana Ciocanea Teodorescu [Universities Leiden and Bordeaux]
Pınar Kılıçer [Universities Leiden and Bordeaux]
Chloë Martindale [Universities Leiden and Bordeaux]
Emmanouil Tzortzakis [Universities Leiden and Bordeaux]
Athanasios Angelakis [Universities Leiden and Bordeaux, until Jun 2015]

Post-Doctoral Fellows

Cyril Bouvier [Univ. Bordeaux]
Pierre Lezowski [Inria, until Aug 2015]
Sorina Ionica [Univ. Bordeaux, until Aug 2015]

Administrative Assistant

Anne-Laure Gautier [Inria]

Other

Pauline Bert [Inria, Stage Master, from May 2015 until Jul 2015]

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, Karim Belabas, Cyril Bouvier, Julio Brau Avila, Jean-Paul Cerri, Iuliana Ciocanea Teodorescu, Henri Cohen, Jean-Marc Couveignes, Andreas Enge, Fredrik Johansson, Pınar Kılıçer, Pierre Lezowski.

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 [30] 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, Guilhem Castagnos, Jean-Marc Couveignes, Andreas Enge, Hamish Ivey-Law, Enea Milio, Damien Robert, Emmanouil Tzortzakis.

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 $(\sqrt{q}-1)^{2g}\leqslant|\,\mathrm{Jac}_{\mathcal{C}}\,|\leqslant(\sqrt{q}+1)^{2g}$, or $|\,\mathrm{Jac}_{\mathcal{C}}\,|\approx q^g$, 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 $\mathrm{Jac}_{\mathcal{C}}$, it must be difficult to determine x. Computing x corresponds in fact to computing $\mathrm{Jac}_{\mathcal{C}}$ 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 $\mathrm{Jac}_{\mathcal{C}}$ 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, Fredrik Johansson, Chloë Martindale, Enea Milio, Damien Robert.

Complex multiplication provides a link between number fields and algebraic curves; for a concise introduction in the elliptic curve case, see [32], for more background material, [31]. In fact, for most curves $\mathcal{C}$ over a finite field, the endomorphism ring of $\mathrm{Jac}_{\mathcal{C}}$, 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

The team has been evaluated in 2015, and our scientific project for the next four years has been validated by the external reviewers.

Fredrik Johansson, who was already a postdoc last year, has been recruited as a full time researcher.

The team has organised the Atelier Pari/GP in January 2015 and the ECC 2015 international conference (with a summer school) in September 2015.

Athanasios Angelakis has defended his PhD thesis on *Universal Adelic Groups for Imaginary Quadratic Number Fields and Elliptic Curves* in September 2015.

Julio Brau has defended his PhD thesis on *Galois representations of elliptic curves and abelian entanglements* in December 2015.

Enea Milio has defended his PhD thesis on *Computing modular polynomials in dimension 2* [11] in December 2015.

The European H2020 project OpenDreamKit, in which the team participates, has been accepted.

5. New Software and Platforms

5.1. APIP

Another Pairing Implementation in PARI
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: Jérôme Milan
- URL: http://www.lix.polytechnique.fr/~milanj/apip/apip.xhtml

5.2. Arb

FUNCTIONAL DESCRIPTION

Arb is a C library for arbitrary-precision floating-point ball arithmetic. It supports real and complex numbers, polynomials, power series, matrices, and evaluation of many transcendental functions. All is done with automatic, rigorous error bounds. It has been accepted for inclusion in SageMath.

- Participant: Fredrik Johansson
- Contact: Fredrik Johansson
- URL: http://fredrikj.net/arb/

5.3. AVIsogenies

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

5.4. CM

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.

- Participant: Andreas Enge
- Contact: Andreas Enge
- URL: http://www.multiprecision.org/index.php?prog=cm&page=home

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

5.6. CUBIC

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

5.7. Euclid

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

5.8. GNU MPC

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.

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

5.9. KleinianGroups

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

5.10. MPFRCX

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.

- Participant: Andreas Enge
- Contact: Andreas Enge
- URL: http://www.multiprecision.org/index.php?prog=mpfrcx

5.11. Nemo

FUNCTIONAL DESCRIPTION Nemo is a computer algebra package for the Julia programming language maintained by William Hart with code by William Hart, Tommy Hofmann, Claus Fieker, Fredrik Johansson, Oleksandr Motsak).

The features of Nemo include multiprecision integers and rationals, integers modulo n, p-adic numbers, finite fields (prime and non-prime order), number field arithmetic, maximal orders of number fields, arithmetic of ideals in maximal orders, arbitrary precision real and complex balls, generic polynomials, power series, fraction fields, residue rings and matrices.

- Participant: Fredrik Johansson
- Contact: William Hart
- URL: http://nemocas.org/

5.12. PARI/GP

FUNCTIONAL DESCRIPTION

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.

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

6. New Results

6.1. Class groups and other invariants of number fields

Participants: Karim Belabas, Jean-Paul Cerri, Henri Cohen, Pınar Kılıçer, Pierre Lezowski.

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. The paper [14] by Henri Cohen, Simon Rubinstein-Salzedo and Frank Thorne proves an identity relating certain degree fields with Galois groups D and F, respectively, for any odd prime, giving another proof of the Ohno–Nakagawa relation between the counting functions of certain cubic fields.

Pınar Kılıçer and Marco Streng have solved a variant of the class number 1 problem for quartic CM fields with a geometric motivation [27]; the question is whether a certain class group is trivial, which corresponds to a genus 2 curve with that complex multiplication being defined over a real-quadratic number field (instead of an extension). Using classical techniques provides a bound on the discriminant of such fields, which they refine taking ramification into account to obtain a practically useful bound. A carefully crafted enumeration algorithm finishes the proof.

In the article [28], P. Lezowski studies the Euclidean properties of matrix algebras $M_n(R)$ over commutative rings R. In particular, he shows that for any integer $n > 1$, $M_n(R)$ is a left and right Euclidean ring if and only if R is principal. The proof is constructive and allows to better understand the Euclidean order types of matrix algebras. Similar ideas are also applied to prove k-stage Euclidean properties of $M_n(R)$, linking them with Bézout property for the ring R. The article [28] has been submitted to *Journal of Algebra*.

The article by Aurel Page on the computation of arithmetic Kleinian groups has appeared [21].

6.2. Complex L-functions and certified arithmetic

Participants: Bill Allombert, Karim Belabas, Henri Cohen, Fredrik Johansson.

Fredrik Johansson's paper [23] has been published and presented at the 22nd IEEE Symposium on Computer Arithmetic (ARITH22), Lyon, France. This paper describes a new implementation of the elementary transcendental functions exp, sin, cos, log and atan for variable precision up to approximately 4096 bits. Compared to the MPFR library, it achieves a maximum speedup ranging from a factor 3 for cos to 30 for atan.

Bill Allombert, Karim Belabas, Henri Cohen and Pascal Molin (Paris 7) have implemented a new framework in PARI/GP to compute and manipulate complex L-functions and the associated ϑ and Λ functions, exporting 25 new functions to the GP computer algebra system.

6.3. Elliptic curve and Abelian varieties cryptology

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

In [29] David Lubicz and Damien 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 cryptosystems based on abelian varieties. Depending on the cryptographic application, the speed record holders 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 problem in certain cryptographic protocols. The previous known models to work on the Jacobian rather than the Kummer surface (Mumford coordinates or the 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 addition), and uses it to speed up multi-exponentiations in Kummer varieties and to obtain new models of abelian surfaces in which the scalar multiplication is as fast as on the Kummer surface. This paper was written last year but heavily revised in 2015 and has been accepted (up to minor revisions) in the journal Finite Fields and Their Applications.

The paper [19] by David Lubicz and Damien Robert about computing certain isogenies in quasi optimal time has been published in the LMS Journal of Computation and Mathematics and the paper [18] by the same authors about optimal pairing computation on abelian varieties has been published in the Journal of Symbolic Computation. This paper expands the article [15] by Romain Cosset and Damien Robert about the computation of (ℓ, ℓ)-isogenies in dimension 2 which has been published in Mathematics of Computation.

Enea Milio has published one of the main results of his PhD thesis [20]. He has generalised the work of Régis Dupont for computing modular polynomials in dimension 2 to new invariants. He describes an algorithm to compute modular polynomials for invariants derived from theta constants and proves under some heuristics that this algorithm is quasi-linear in its output size. Some properties of the modular polynomials defined from quotients of theta constants are analysed and experiments with an implementation are related.

The paper [16] by Jean-Marc Couveignes and Tony Ezome explaining how to efficiently evaluate functions, including Weil functions and canonical theta functions, on Jacobian varieties and their quotients has been published in the LMS Journal of Computation and Mathematics. This paper also describes 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 [26], Sorina Ionica and Emmanuel Thomé look at the structure of isogeny graphs of genus 2 Jacobians with maximal real multiplication. They generalise a result of Kohel's describing the structure of the endomorphism rings of the isogeny graph of elliptic curves. Their setting considers genus 2 jacobians with complex multiplication, with the assumptions that the real multiplication subring is maximal and has class number 1. Over finite fields, they derive a depth first search algorithm for computing endomorphism rings locally at prime numbers, if the real multiplication is maximal.

6.4. Cryptology with quadratic fields

Participant: Guilhem Castagnos.

In [22] Guilhem Castagnos and Fabien Laguillaumie design a linearly homomorphic encryption scheme the security of which relies on the hardness of the decisional Diffie-Hellman problem. The approach requires some special features of the underlying group. In particular, its order is unknown and it contains a subgroup in which the discrete logarithm problem is tractable. Therefore, their instantiation holds in the class group of a non-maximal order of an imaginary quadratic field. Its algebraic structure makes it possible to obtain such a linearly homomorphic scheme in which the message space is the whole set of integers modulo a prime p and which supports an unbounded number of additions modulo p from the ciphertexts. A notable difference with previous work is that, for the first time, the security does not depend on the hardness of the factorisation of integers. As a consequence, under some conditions, the prime p can be scaled to fit the application needs. This paper has beenpresented at the cryptographer's track at the RSA Conference 2015.

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR Peace – Parameter spaces for Efficient Arithmetic and Curve security Evaluation

Participants: Bill Allombert, Karim Belabas, Jean-Marc Couveignes, Andreas Enge, Hamish Ivey-Law, Enea Milio, 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".

7.1.2. ANR Simpatic – SIM and PAiring Theory for Information and Communications security

Participants: Guilhem Castagnos, Damien Robert, Sorina Ionica, Cyril Bouvier.

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.

G. Castagnos is a participant in the Task 4 whose role is to design new cryptographic primitives adapted to the specific applications of the Simpatic Project.

7.2. European Initiatives

7.2.1. FP7 & H2020 Projects

7.2.1.1. ANTICS

Title: Algorithmic Number Theory in Computer Science

Programm: FP7

Duration: January 2012 - December 2016

Coordinator: Inria

Inria contact: Andreas Enge

'During the past twenty years, we have witnessed profound technological changes, summarised under the terms of digital revolution or entering the information age. It is evident that these technological changes will have a deep societal impact, and questions of privacy and security are primordial to ensure the survival of a free and open society. Cryptology is a main building block of any security solution, and at the heart of projects such as electronic identity and health cards, access control, digital content distribution or electronic voting, to mention only a few important applications. During the past decades, public-key cryptology has established itself as a research topic in computer science; tools of theoretical computer science are employed to "prove" the security of cryptographic primitives such as encryption or digital signatures and of more complex protocols. It is often forgotten, however, that all practically relevant public-key cryptosystems are rooted in pure mathematics, in particular, number theory and arithmetic geometry. In fact, the socalled security "proofs" are all conditional to the algorithmic untractability of certain number theoretic problems, such as factorisation of large integers or discrete logarithms in algebraic curves. Unfortunately, there is a large cultural gap between computer scientists using a black-box security reduction to a supposedly hard problem in algorithmic number theory and number theorists, who are often interested in solving small and easy instances of the same problem. The theoretical grounds on which current algorithmic number theory operates are actually rather shaky, and cryptologists are generally unaware of this fact. The central goal of ANTICS is to rebuild algorithmic number theory on the firm grounds of theoretical computer science.'

7.2.1.2. Open Dream Kit

Title: Algorithmic Number Theory in Computer Science

Programm: FP7

Duration: September 2015 - August 2019

Inria contact: Karim Belabas

OpenDreamKit is a Horizon 2020 European Research Infrastructure project (#676541, call e-infrastructures for virtual research environments) that will run for four years, starting from September 2015. It will provide 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.

From this ecosystem, OpenDreamKit will deliver a flexible toolkit enabling research groups to set up Virtual Research Environments, customised to meet the varied needs of research projects in pure mathematics and applications, and supporting the full research life-cycle from exploration, through proof and publication, to archival and sharing of data and code.

The project involves about 50 people spread over 15 sites in Europe, with a total budget of about 7.6 million euros. The largest portion of that will be devoted to employing an average of 11 researchers

and developers working full time on the project. Additionally, the participants will contribute the equivalent of six other people working full time.

Countries involved include France (Universités Paris-Sud, Versailles, Bordeaux, Grenoble and the industrial partner Logilab), Germany (Kaiserslautern, Bremen), United Kingdom (Oxford, Southampton, Sheffield, St Andrews, Warwick), Norway (Simula), Poland (University Silesia), Switzerland (University Zürich).

7.3. International Initiatives

7.3.1. 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 (EMA) in Libreville with the International Center for Pure and Applied Mathematics (ICPAM/CIMPA), March 2015, attended by most of the members of Macisa;
- The visit of Abdoul Aziz Ciss (Dakar) and Emmanuel Fouotsa (Bamenda) to Bordeaux, September 2015, for the Elliptic Curve Cryptography and Summer School conference;
- The visit of Tony Ezome to Bordeaux, October 2015;
- The visit of Damien Robert to Yaoundé, Cameroun, to give courses on cryptography for a special seminar on security event.

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

Researchers visiting the team to give a talk to the team seminar include David Kohel (Université d'Aix-Marseille), Tony Ezome (Université des Sciences et Techniques de Masuku, Franceville), Abdoul Aziz Ciss (Ecole Polytechnique de Thiès, Sénégal), Emmanuel Fouotsa (École Normale Supérieure de l'Université de Bamenda), Renate Scheidler (University Calgary), Eduardo Friedman (Universidad de Chile), Benjamin Smith (Inria & LIX, École Polytechnique), Bernadette Perrin-Riou (Paris-Sud).

The visit of Ciss, Ezome and Fouotsa were also part of the collaboration through the Macisa team.

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events organisation

The team has organised the international conference ECC 2015 — 19th Workshop on Elliptic Curve Cryptography in Bordeaux from September 28 to September 30 and a Summer School on elliptic curves the week before from September 23 to September 25.

The three day conference with 170 participants comprised about fifteen invited lectures by world-renowned scientist, presenting the major advances of the previous year. Topics ranged widely from new mathematical and algorithmic results on elliptic curves and abelian varieties, over implementations and attacks of cryptosystems up to practical studies on real-world use of curve based cryptography. This year, a panel discussion on the standardisation of elliptic curves for cryptographic use was also organised.

The preceding summer school with about 70 participants included four invited lectures of three hours each (one of which was given by Damien Robert), and a software tutorial on Sage and Pari/GP. The tutorial on Pari/GP was done by Bill Allombert and Karim Belabas. The school concluded with an afternoon of computer exercices.

8.1.1.1. General chair, scientific chair

Andreas Enge and Damien Robert were scientific chairs, Andreas Enge was the general chair.

8.1.1.2. Member of the organizing committees

Andreas Enge, Anne-Laure Gautier and Damier Robert were members of the organizing committee.

8.1.2. Scientific events selection

8.1.2.1. Chair of conference program committees

- Andreas Enge was the programme chair of ECC 2015 (Bordeaux)

8.1.2.2. Member of the conference program committees

- Damien Robert was a member of the ECC 2015 (Bordeaux), Asiacrypt 2015 (Auckland) and CRI 2015 (Yaoundé) program committees.
- Sorina Ionica was a member of the Latincrypt 2015 (Guadalajara, Mexico) program committee.

8.1.3. Journal

8.1.3.1. 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.

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.

8.1.4. Invited talks

- F. Johansson gave an invited talk on "Fast arbitrary-precision evaluation of special functions in the Arb library" at The 13th International Symposium on Orthogonal Polynomials, Special Functions and Applications (OPSFA-13), National Institute of Standards and Technology, Gaithersburg, MD, USA (June 2015)
- S. Ionica gave an invited talk on “Fast scalar multiplicaton in pairing groups” at the "Pairings in cryptography" Minisymposium, SIAM AG15 Conference, Daejeon, South Korea (August 2015)
- A. Enge gave an invited talk on “Computing with theta functions on abelian surfaces” at the 11th Symposium on Algebra and Computation (AC2015), Tokyo Metropolitan University (December 2015)
- E. Milio gave an invited talk on “Computation of modular polynomials in dimension 2” at the Elliptic Curve Cryptography 2015 Conference in Bordeaux (September 2015). He also gave a similar talk at the Journées codage et cryptographie at la Londe-les-Maures (October 2015).
- D. Robert gave two invited talks on “Isogenies, Polarisations and Real Multiplication”, one for the Modular Forms and Curves of Low Genus: Computational Aspects conference at Providence (September 2015) and one for the Journées codage et cryptographie at la Londe-les-Maures (October 2015).

8.1.5. Scientific expertise

J.-M. Couveignes is a member of the scientific council of the labex "Fondation Sciences Mathématiques de Paris", FSMP, Paris.

J.-M. Couveignes is a member of the ’conseil d’orientation’ of the labex "Institut de Recherche en Mathématiques, Interactions et Applications", IRMIA, Strasbourg.

8.1.6. Research administration

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.

Since January 2015, J.-M. Couveignes is the head of the Math Institute (IMB).

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

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence: Enea Milio, Analyse, 12h, L1, Université de Bordeaux, France;

Licence: Enea Milio, Mise à niveau Maths, 12h, L1, Université de Bordeaux, France;

Licence: G. Castagnos, *Algorithmique algébrique 1*, 34.67h, L3, University of Bordeaux, France

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*, 30h, M2, University of Bordeaux, France;

Master: K. Belabas, *Computational number theory*, 70h, M2, University of Bordeaux, France;

Master: K. Belabas, *Computer Algebra*, 90h, M2, University of Bordeaux, France;

Master: K. Belabas, *Algorithms for Public Key Cryptography*, 30h, M2, University of Bordeaux, France;

Summer School: F. Johansson gave three invited lectures on "High-precision methods for zeta functions" at the UNCG Summer School in Computational Number Theory, Greensboro, NC, USA in May 2015;

Summer School: J.-M. Couveignes and D. Robert gave a one week course on *Algorithmic number theory and cryptology* for the École Mathématique Africaine, organised with support from the Centre International de Mathématiques Pures et Appliquées (CIMPA) in March 2015 at Franceville, Gabon.

Summer School: D. Robert gave a talk on *The group structure of rational points of elliptic curves over a finite field* (including practical exercices on Sage or Pari/GP) for the Elliptic Curves Cryptography (ECC 2015) Summer School in September 2015 at Bordeaux.

Summer School: D. Robert gave a one week course on *Introduction to cryptology* as part of the seminar on security at Yaoundé I University preceding the Colloque de Recherche en Informatique in December 2015.

Summer School: S. Ionica gave a two lecture course on *Introduction to elliptic curve cryptography* at the ASCrypto 2015, the summer school organised at the Latincrypt 2015 conference, in Guadalajara, Mexico.

Summer School: A. Enge gave eight lectures at the SEAMS school on *Algebras and their applications (Quantum Physics, Cryptography and Statistics)* at Universiti Putra Malaysia in November 2015, entitled *Elliptic curves* (two lectures), *Hyperelliptic curves* (two lectures), *Kummer varieties*, *Exponential and subexponential algorithms for the discrete logarithm problem* (two lectures), *Pairings on elliptic curves*.

8.2.2. Supervision

PhD: Athanasios Angelakis, *Universal Adelic Groups for Imaginary Quadratic Number Fields and Elliptic Curves*, University of Bordeaux / University of Leiden, supervised by K. Belabas and P. Stevenhagen, defended 09/2015.

PhD: Julio Brau, *Galois representations of elliptic curves and abelian entanglements*, University of Bordeaux / University of Leiden, supervised by K. Belabas and P. Stevenhagen, defended 12/2015.

PhD: Enea Milio, *Computing modular polynomials in dimension 2*, University Bordeaux, supervised by A. Enge and D. Robert, defended 12/2015.

PhD in progress: Iuliana Ciocanea, *The module isomorphism problem*, supervised by K. Belabas and H. Lenstra.

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

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, P. Stevenhagen, M. Streng

F. Johansson was a mentor in Google Summer of Code for Anubhav Srivastava (undergraduate student at IIIT Hyderabad) who did a successful GSoC project on "BLAS wrappers for linear algebra in FLINT"

S. Ionica supervised P. Bert's Master 1 thesis "Index calculus algorithms for small genus hyperelliptic curves". P. Bert is a student of the CSI master (Univ. of Bordeaux) and was an intern with LFANT from the 10th of May 2015 to the 31th of July 2015.

8.2.3. Juries

K. Belabas was a member of the jury of Olga Balkanova's PhD defense in Bordeaux (supervised by G. Molteni and G. Ricotta)

K. Belabas was a member (as supervisor) of the juries of Athanasios Angelakis and Julio Brau.

J.-M. Couveignes was a member of the jury, as a referee, for François Arnaud's HDR defense.

J.-M. Couveignes was a member of the jury, for Cyril Bouvier's PhD defense.

J.-M. Couveignes was a member of the jury, for Tristan Vaccon's PhD defense.

J.-M. Couveignes was a member of the jury, for Kevin Atighehchi's PhD defense.

A. Enge and D. Robert were members (as supervisors) of the jury for Enea Milio's PhD defense.

8.3. Popularization

Damien Robert participated in a CinémaScience event to discuss with the public after a projection of the film "Imitation Game" on Alan Turing. The theme of the intervention was "The contributions of Alan Turing from computer science to cryptography".

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] 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-Verlag, New 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 & Hall, Boca 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° 1, pp. 24–41

[10] D. LUBICZ, D. ROBERT. *Computing isogenies between abelian varieties*, in "Compositio Mathematica", 09 2012, vol. 148, n° 05, pp. 1483–1515, http://dx.doi.org/10.1112/S0010437X12000243

Publications of the year

Doctoral Dissertations and Habilitation Theses

[11] E. MILIO. *Computing modular polynomials in dimension 2*, université de bordeaux, December 2015, https://tel.archives-ouvertes.fr/tel-01240690

Articles in International Peer-Reviewed Journals

[12] 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

[13] H. COHEN. *Exact counting of D_ℓ number fields with given quadratic resolvent*, in "Mathematics of Computation", 2015, vol. 84, n° 294, pp. 1933-1951, https://hal.archives-ouvertes.fr/hal-01027417

[14] H. COHEN, S. RUBINSTEIN-SALZEDO, F. THORNE. *Identitites for Field Extensions Generalizing the Ohno–Nakagawa Relations*, in "Compositio Mathematica", 2015, vol. 151, n° 11, pp. 2059-2075, https://hal.inria.fr/hal-01109980

[15] R. COSSET, D. ROBERT. *Computing (l,l)-isogenies in polynomial time on Jacobians of genus 2 curves*, in "Mathematics of Computation", 2015, vol. 84, n° 294, pp. 1953-1975, Accepté pour publication à Mathematics of Computations [*DOI :* 10.1090/S0025-5718-2014-02899-8], https://hal.archives-ouvertes.fr/hal-00578991

[16] J.-M. COUVEIGNES, T. EZOME. *Computing functions on Jacobians and their quotients*, in "The London Mathematical Society Journal of Computations and Mathematics", October 2015, vol. 18, n° 1, pp. 555-577, https://hal.archives-ouvertes.fr/hal-01088933

[17] A. ENGE. *Bilinear pairings on elliptic curves*, in "L'Enseignement Mathématique", 2015, vol. 61, n° 2, pp. 209–241, https://hal.inria.fr/hal-00767404

[18] 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

[19] D. LUBICZ, D. ROBERT. *Computing separable isogenies in quasi-optimal time*, in "LMS Journal of Computation and Mathematics", 2015, vol. 18, n° 1, pp. 198-216 [*DOI :* 10.1112/S146115701400045X], https://hal.archives-ouvertes.fr/hal-00954895

[20] E. MILIO. *A quasi-linear time algorithm for computing modular polynomials in dimension 2*, in "LMS Journal of Computation and Mathematics", 2015, vol. 18, pp. 603-632, https://hal.archives-ouvertes.fr/hal-01080462

[21] A. PAGE. *Computing arithmetic Kleinian groups*, in "Mathematics of Computation", 2015, vol. 84, n° 295, pp. 2361-2390, https://hal.archives-ouvertes.fr/hal-00703043

International Conferences with Proceedings

[22] G. CASTAGNOS, F. LAGUILLAUMIE. *Linearly Homomorphic Encryption from DDH*, in "The Cryptographer's Track at the RSA Conference 2015", San Francisco, United States, Topics in Cryptology — CT-RSA 2015, April 2015, n° 9048 [*DOI :* 10.1007/978-3-319-16715-2_26], https://hal.archives-ouvertes.fr/hal-01213284

[23] F. JOHANSSON. *Efficient implementation of elementary functions in the medium-precision range*, in "22nd IEEE Symposium on Computer Arithmetic (ARITH22)", Lyon, France, June 2015 [*DOI :* 10.1109/ARITH.2015.16], https://hal.archives-ouvertes.fr/hal-01079834

Patents and standards

[24] G. ZEMOR, L. JUAN, J.-M. CAMUS, M. PERRET, J.-M. COUVEIGNES. *Method and device for protecting the integrity of data transmitted over a network*, April 2015, n° US 9,009,839 B2, https://hal.archives-ouvertes.fr/hal-01213785

Other Publications

[25] J. BRAU, N. JONES. *Elliptic curves with 2-torsion contained in the 3-torsion field*, January 2015, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01111744

[26] S. IONICA, E. THOMÉ. *Isogeny graphs with maximal real multiplication*, January 2015, working paper or preprint, https://hal.archives-ouvertes.fr/hal-00967742

[27] P. KILIÇER, M. STRENG. *The CM class number one problem for curves of genus 2*, December 2015, working paper or preprint, https://hal.inria.fr/hal-01248630

[28] P. LEZOWSKI. *On some Euclidean properties of matrix algebras*, March 2015, 39 pages, some corrections and improvements, especially in Section 7, https://hal.archives-ouvertes.fr/hal-01135202

[29] D. LUBICZ, D. ROBERT. *Arithmetic on Abelian and Kummer Varieties*, September 2015, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01057467

References in notes

[30] 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

[31] 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

[32] 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/