IN PARTNERSHIP WITH:
CNRS

Université de Bordeaux

Activity Report 2019

Project-Team LFANT

Lithe and fast algorithmic number theory

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

RESEARCH CENTER
Bordeaux - Sud-Ouest

THEME
Algorithmics, Computer Algebra and Cryptology

Table of contents

Project-Team LFANT

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

Keywords:

Computer Science and Digital Science:

A4.3.1. - Public key cryptography
A8.4. - Computer Algebra
A8.5. - Number theory
A8.10. - Computer arithmetic

Other Research Topics and Application Domains:

B6. - IT and telecom
B9.5.2. - Mathematics

1. Team, Visitors, External Collaborators

Research Scientists

Andreas Enge [Team leader, Inria, Senior Researcher, HDR]
Razvan Barbulescu [CNRS, Researcher, from Sep 2019]
Xavier Caruso [CNRS, Senior Researcher, HDR]
Fredrik Johansson [Inria, Researcher]
Aurel Page [Inria, Researcher]
Damien Robert [Inria, Researcher]

Faculty Members

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

PhD Students

Jared Guissmo Asuncion [Univ de Bordeaux, PhD Student]
Amaury Durand [Univ de Bordeaux, PhD Student, from Sep 2019]
Elie Eid [Univ de Rennes I, PhD Student]
Jean Kieffer [École Normale Supérieure de Paris, PhD Student]
Abdoulaye Maiga [Senegal, PhD student]
Pavel Solomatin [Leiden University, PhD Student]
Ida Tucker [École Normale Supérieure de Lyon, PhD Student]
Anne Edgar Wilke [Inria, PhD Student, from Sep 2019]

Technical staff

Bill Allombert [CNRS, Engineer]

Administrative Assistant

Sabrina Duthil [Inria, Administrative Assistant]

External Collaborator

Tony Ezome Mintsa [Universite des Sciences et Techniques de Masuku, Gabon]

2. Overall Objectives

2.1. Presentation

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

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

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

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

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

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

3. Research Program

3.1. Number fields, class groups and other invariants

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

Modern number theory has been introduced in the second half of the 19th century by Dedekind, Kummer, Kronecker, Weber and others, motivated by Fermat's conjecture: There is no non-trivial solution in integers to the equation $x^n + y^n = z^n$ for $n \geqslant 3$. 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 [36] for a recent account.

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

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

3.2. Function fields, algebraic curves and cryptology

Participants: Karim Belabas, Guilhem Castagnos, Jean-Marc Couveignes, Andreas Enge, Damien Robert, Jean Kieffer, Razvan Barbulescu.

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: Jared Guissmo Asuncion, Karim Belabas, Henri Cohen, Jean-Marc Couveignes, Andreas Enge, Fredrik Johansson, Chloe Martindale, Damien Robert.

Complex multiplication provides a link between number fields and algebraic curves; for a concise introduction in the elliptic curve case, see [38], for more background material, [37]. 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

Guilhem Castagnos defended his professorial degree ("habilitation à diriger des recherches") on the topic of *Cryptography based on quadratic fields: cryptanalyses, primitives and protocols*[11].

4.1.1. Awards

Fredrik Johansson won the best paper award at the conference ARITH26 — 26th IEEE Symposium on Computer Arithmetic in Kyoto for his contribution on dot products and matrix multiplication in arbitrary precision .

BEST PAPER AWARD:

[21]
F. JOHANSSON. *Faster arbitrary-precision dot product and matrix multiplication*, in "26th IEEE Symposium on Computer Arithmetic (ARITH26)", Kyoto, Japan, June 2019, https://arxiv.org/abs/1901.04289 , https://hal.inria.fr/hal-01980399

5. New Software and Platforms

5.1. APIP

Another Pairing Implementation in PARI

KEYWORDS: Cryptography - Computational number theory

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

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

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

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

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

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

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

5.2. AVIsogenies

Abelian Varieties and Isogenies

KEYWORDS: Computational number theory - Cryptography

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

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

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

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

5.3. CM

KEYWORD: Arithmetic

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

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

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

5.4. CMH

Computation of Igusa Class Polynomials

KEYWORDS: Mathematics - Cryptography - Number theory

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

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

5.5. CUBIC

KEYWORD: Number theory

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

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

5.6. Euclid

KEYWORD: Number theory

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

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

5.7. KleinianGroups

KEYWORDS: Computational geometry - Computational number theory

FUNCTIONAL DESCRIPTION: KleinianGroups is a Magma package that computes fundamental domains of arithmetic Kleinian groups.

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

5.8. GNU MPC

KEYWORD: Arithmetic

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

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

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

5.9. MPFRCX

KEYWORD: Arithmetic

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

RELEASE FUNCTIONAL DESCRIPTION: - new function `product_and_hecke` - improved memory consumption for unbalanced FFT multiplications

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

5.10. PARI/GP

KEYWORD: Computational number theory

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

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

5.11. Platforms

5.11.1. SageMath

Following the article [19], Xavier Caruso and Thibaut Verron proposed an implementation of Tate algebras and ideals in Tate algebras (including an implementation of Buchberger algorithm) for SageMath; their implementation is now part of the standard distribution.

Xavier Caruso implemented a new unified framework for dealing with ring extensions and field extensions in SageMath. This code will be integrated soon in the standard distribution.

5.11.2. ARB

Fredrik Johansson released a new version, 2.17, of ARB.

6. New Results

6.1. Cryptographic Protocols

Participants: Guilhem Castagnos, Ida Tucker.

In [20], G. Castagnos, D. Catalano, F. Laguillaumie, F. Savasta and I. Tucker propose a new cryptographic protocol to compute ECDSA signatures with two parties.

ECDSA (Elliptic Curves Digital Signature Algorithm) is a widely adopted standard for electronic signatures. For instance, it is used in the TLS (Transport Layer Security) protocol and in many cryptocurrencies such as Bitcoin. For cryptocurrencies, ECDSA is used in order to sign the transactions: if Alice wants to give n bitcoins to Bob, she uses her secret key to sign with ECDSA a bit string encoding this information.

As a result, if the secret key of Alice is stolen, for example if her computer is compromised, an attacker can stole all her bitcoins. A common solution to this problem is to share the key on multiple devices, for example a laptop and a mobile phone. Both devices must collaborate in order to issue a signature, and if only one device is compromised, no information on the key is leaked. This setting belongs to the area of secure multiparty computation.

There have been recent proposals to construct 2 party variants of ECDSA signatures but constructing efficient protocols proved to be much harder than for other signature schemes. The main reason comes from the fact that the ECDSA signing protocol involves a complex equation compared to other signatures schemes. Lindell recently managed to get an efficient solution using the linearly homomorphic cryptosystem of Paillier. However his solution has some drawbacks, for example the security proof resorts to a non-standard interactive assumption.

By using another approach based on hash proofs systems we obtain a proof that relies on standard assumptions. Moving to concrete constructions, we show how to instantiate our framework using class groups of imaginary quadratic fields. Our implementations show that the practical impact of dropping such interactive assumptions is minimal. Indeed, while for 128-bit security our scheme is marginally slower than Lindell's, for 256-bit security it turns out to be better both in key generation and signing time. Moreover, in terms of communication cost, our implementation significantly reduces both the number of rounds and the transmitted bits without exception.

This paper was presented at the CRYPTO Conference 2019, and is part of the ALAMBIC project.

6.2. Coding Theory

Participants: Xavier Caruso, Aurel Page.

In [29], Xavier Caruso developed a theory of residues for skew rational functions (which are, by definition, the quotients of two skew polynomials), proving in particular a skew analogue of the residue formula and a skew analogue of the classical formula of change of variables for residues. He then used his theory to define and study a linearized version of Goppa codes. He showed that these codes meet the Singleton bound (for the sum-rank metric) and are the duals of the linearized Reed–Solomon codes defined recently by Martínez-Peñas. Efficient encoding and decoding algorithms are also designed.

C. Maire and A. Page updated the preprint *Error-correcting codes based on non-commutative algebras* [33] according to the comments of referees.

6.3. Number fields

Participants: Razvan Barbulescu, Jean-Marc Couveignes, Jean-Paul Cerri, Pierre Lezowski.

In [30], Jean-Marc Couveignes constructs small models of number fields and deduces a better bound for the number of number fields of given degree n and discriminant bounded by H. This work improves on previous results by Schmidt and Ellenberg-Venkatesh. Schmidt obtains a bound $H^{\frac{n+2}{4}}$ times a function of n. Ellenberg and Venkatesh obtain a bound $H^{\exp(O(\sqrt{\log n}))}$ times a function of n. The new idea is to combine geometry of numbers and interpolation theory to produces small projective models and lower the exponent of H down to $O(\log^3 n)$. A key point is to look for local equations rather than a full set of generators of the ideal of these models.

In [12], Razvan Barbulescu in a joint work with Jishnu Ray (University of British Columbia, Vancouver) brings elements to support Greenberg's p-rationality conjecture. On the theoretical side, they propose a new family proven to be p-rational. On the algorithmic side, the compare the tools to enumerate number fields of given abelian Galois group and of computing class numbers, and extend the experiments on the Cohen-Lenstra-Martinet conjectures.

In collaboration with Pierre Lezowski, Jean-Paul Cerri has studied in [15] norm-Euclidean properties of totally definite quaternion fields over number fields. Building on their previous work about number fields, they have proved that the Euclidean minimum and the inhomogeneous minimum of orders in such quaternion fields are always equal. Additionally, they are rational under the hypothesis that the base number field is not quadratic. This single remaning open case corresponds to the similar open case remaining for real number fields.

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

6.4. Modular forms and L-functions

Participant: Henri Cohen.

Members of the team have taken part in an international autumn school on computational number theory at the Izmir Institute of Technology (IZTECH) in 2017. Henri Cohen has transformed his two lectures in book chapters. The text on modular forms [23] presents the (of course extremely condensed) view of the book [6] he has coauthored. The chapter on L-functions [24] is closely related to new developments in PARI/GP.

In [25] the same author explains how to compute Fourier expansions at all cusps of any modular form of integral or half-integral weight thanks to a theorem of Borisov–Gunnells and explicit expansions of Eisenstein series at all cusps. Using this, he gives a number of methods for computing arbitrary Petersson products. Implementations in our PARI/GP software are also described.

A complementary approach using modular symbols is used in [14] by Karim Belabas, Dominique Bernardi and Bernadette Perrin-Riou to compute Manin's constant and the modular degree of elliptic curves defined over $\mathbb{Q}$.

6.5. p-adic rings and geometry

Participant: Xavier Caruso.

In [19], Xavier Caruso, Tristan Vaccon and Thibaut Verron laid the foundations of an algorithmic treatment of rigid p-adic geometry by introducting and studing Gröbner bases over Tate algebras. In addition, they designed a Buchberger-like and a F4-like algorithm for computing such Gröbner bases.

In [22], Xavier Caruso presents a survey on Fontaine's theory of p-adic period rings. These notes are based on a course given jointly by Laurent Berger and Xavier Caruso in Rennes in 2014; their aim is to detail the construction of the rings B_{crys} and B_{dR} (and some of their variants) and state several comparison theorems between étale and crystalline or de Rham cohomologies for p-adic algebraic varieties.

6.6. Geometry

Participant: Aurel Page.

The paper [13], *Can you hear the homology of 3-dimensional drums?* by A. Bartel and A. Page was published in Commentarii Mathematici Helvetici.

6.7. Complex multiplication of abelian varieties and elliptic curves

Participants: Razvan Barbulescu, Sorina Ionica, Chloe Martindale, Enea Milio, Damien Robert.

In [16], Sorina Ionica, former postdoc of the team, 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.

Antonin Riffaut examines in [18] whether there are relations defined over $\mathbb{Q}$ that link (additively or multiplicatively) different singular moduli $j(\tau)$, invariants of elliptic curves with complex multiplication by different quadratic rings.

In [34], Chloe Martindale presents an algorithm to compute higher dimensional Hilbert modular polynomials. She also explains applications of this algorithm to point counting, walking on isogeny graphs, and computing class polynomials.

In [28], Razvan Barbulescu and Sudarshan Shinde (Sorbonne Université) make a complete list of the 1525 infinite families of elliptic curves without CM which have a particular behaviour in the ECM factoring algorithm, the 20 previously known families having been found by ad-hoc methods. The new idea was to use the characterisation of ECM-friendly families in terms of their Galois image and to use the recent progress in the topic of Mazur's program. In particular, for some of the families mentioned theoretical in the literature the article offers the first publication of explicite equations.

E. Milio and D. Robert updated their paper [35] on computing cyclic modular polynomials.

6.8. Pairings

Participant: Razvan Barbulescu.

In [27], Razvan Barbulescu in a joint work with Nadia El Mrabet (École des Mines de Saint-Étienne) et Loubna Ghammam (Bosch) makes a review of the families of elliptic curves for pairing-based cryptology. This was necessary after the invention of a new variant of the NFS algorithm in 2016 by Barbulescu and Taechan Kim, which showed that the previously used key sizes for pairings were insecure. The novelty of this review article is double : first they consider a large number of families, some of which were never analysed in the literature because they were not likely to be the best and secondly they combine in the same article the security analysis of each family with a non-optimized implementation. This allows the industry to select a different family for each type of utilisation of pairings.

6.9. Multiprecision arithmetic

Participant: Fredrik Johansson.

In [17], F. Johansson and I. Blagouchine devise an efficient algorithm to compute the generalized Stieltjes constants $\gamma_n(a)$ to arbitrary precision with rigorous error bounds, for the first time achieving this with low complexity with respect to the order n. The algorithm consists of locating an approximate steepest descent contour and then evaluating the integral numerically in ball arithmetic using the Petras algorithm with a Taylor expansion for bounds near the saddle point. An implementation is provided in the Arb library.

In [26], F. Johansson describes algorithms to compute elliptic functions and their relatives (Jacobi theta functions, modular forms, elliptic integrals, and the arithmetic-geometric mean) numerically to arbitrary precision with rigorous error bounds for arbitrary complex variables. Implementations in ball arithmetic are available in the Arb library. This overview article discusses the standard algorithms from a concrete implementation point of view, and also presents some improvements.

In [21], Fredrik Johansson develops algorithms for real and complex dot product and matrix multiplication in arbitrary-precision floating-point and ball arithmetic. The new methods are implemented in Arb and significantly speed up polynomial operations and linear algebra in high precision.

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR Alambic – AppLicAtions of MalleaBIlity in Cryptography

Participant: Guilhem Castagnos.

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

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

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

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

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

Participants: Xavier Caruso, Jean-Marc Couveignes.

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

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

1. draw a conjectural picture of the (still hypothetical) p-adic Langlands correspondence in the case of GL_n,
2. compute many deformation spaces of Galois representations and make the bridge with deformation spaces of representations of reductive groups,
3. design new algorithms for computations with Hilbert and Siegel modular forms and their associated Galois representations.

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

7.1.3. ANR Ciao – Cryptography, Isogenies and Abelian varieties Overwhelming

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

The CIAO ANR project is a young researcher ANR project led by Damien Robert October 2019.

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

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

Applications of this project is to improve the security of communications in a context where the currently used cryptosystems are vulnerable to quantum computers. Beyond post-quantum cryptography, isogeny based cryptosystems also allow to construct new interesting cryptographic tools, like Verifiable Delay Functions, used in block chains.

7.2. European Initiatives

7.2.1. FP7 & H2020 Projects

Title: OpenDreamKit

Program: H2020

Duration: January 2016 - December 2019

Coordinator: Nicolas Thiéry

Inria contact: Karim Belabas

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

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

7.3. International Initiatives

7.3.1. Inria International Labs

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

7.3.1.1. FAST

Title: (Harder Better) FAster STronger cryptography

International Partner (Institution - Laboratory - Researcher): and the PRMAIS project
Université des Sciences et Techniques de Masuku (Gabon) - Tony Ezome

Start year: 2017

See also: http://fast.gforge.inria.fr/

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

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

This was the last year of the Fast projet, which was represented at the Journees du Lirimia in Yaounde by Emmanuel Fouotsa.

In total the project funded one EMA and two CIMPA schools, had 14 publications in journals and conferences (with three upcoming preprints), two PhD defense with two upcoming.

7.3.2. Inria International Partners

7.3.2.1. Informal International Partners

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

Eduardo Friedman (U. of Chile), long term collaborator of K. Belabas's and H. Cohen's, 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 Lubicz (DGA Rennes), Hartmut Monien (Bethe Center for Theoretical Physics, Bonn), Francesco Battestoni (University of Milan), David Roe (MIT, Boston), Maria Dostert (EPFL, Lausanne), and Alice Pellet-Mary (KU Leuven).

Abdoulaye Maiga visited the team for one month in December 2019, and Tony Ezome visited for two weeks in November 2019.

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Journal

8.1.1.1. Member of the Editorial Boards

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

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

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

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

8.1.2. Invited Talks

F. Johansson, *Computing with precision*, Tech Talk, Google X, Mountain View, CA, USA (January 2019)

8.1.3. Scientific Expertise

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

8.1.4. Research Administration

Since January 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 was a member of the "Conseil National des Universités" (25th section, pure mathematics) since 2015 until november 2019.

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

He is a member of the administrative council of the Société Arithmétique de Bordeaux, qui édite le *Journal de théorie des nombres de Bordeaux* et qui soutient des congrès en théorie des nombres.

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.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

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

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

Master: G. Castagnos, *Courbes elliptiques*, 30h, M2, University of Bordeaux, France;

Licence: G. Castagnos, *Arithmétique et Cryptologie*, 24h, L3, Université de Bordeaux, France

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

Master: X. Caruso and J.-M. Couveignes, *Algorithmique arithmétique, introduction à l'algorithmique quantique*, 60h, M2, University of Bordeaux, France;

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

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

Licence : J.-P. Cerri, *Arithmétique et Cryptologie*, TD, 36h, L3, Université de Bordeaux, France

Licence : J.-P. Cerri, *Algèbre linéaire*, TD, 51h, L2, Université de Bordeaux, France

Licence : J.-P. Cerri, *Topologie*, TD, 35h, L3, Université de Bordeaux, France

Master : J.-P. Cerri, *Cryptologie*, Cours-TD, 60h, M1, Université de Bordeaux, France

Licence: J. Kieffer, *Algorithmique Mathématique 2*, 32h, L3, Université de Bordeaux, France

Master: R. Barbulescu, *Arithmetic algorithms for cryptology*, M2, Master Parisien de Recherche Informatique.

Licence, Master : J.-P. Cerri, 2 TER (L3, M1), 1 Projet (M2), Université de Bordeaux, France

Master : J. Asuncion, *Elliptic curves*, TD, 16h, M1, Universiteit Utrecht (Mastermath), Pays-Bas

8.2.2. Supervision

Master thesis: Jean-Raphaël Biehler, *Functional encryption*, supervised by Guilhem Castagnos

Master thesis: Béranger Seguin, *Deformations of Galois representations*, supervised by Xavier Caruso

Master thesis: William Dallaporta, *Parametrization of ideals and other algebraic structures by quadratic forms*, supervised by Karim Belabas

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

PhD in progress: Abdoulaye Maiga, *Computing canonical lift of genus 2 hyperelliptic curves*, University Dakar, supervised by Djiby Sow, Abdoul Aziz Ciss and D. Robert.

PhD in progress: Jared Asuncion, *Class fields of complex multiplication fields*, since September 2017, supervised by A. Enge and Marco Streng (Universiteit Leiden).

PhD in progress: Elie Eid, *Computing isogenies between elliptic curves and curves of higher genus*, since September 2018, supervised by Xavier Caruso and Reynald Lercier

PhD in progress: Amaury Durand, *Geometric Gabidulin codes*, since September 2019, supervised by Xavier Caruso

PhD in progress: Jean Kieffer, *Computing isogenies between abelian surfaces*, since September 2018, supervised by Damien Robert and Aurel Page

PhD in progress: Pavel Solomatin *Topics on L-functions*, since October 2014, supervised by B. de Smit and K. Belabas.

PhD in progress: Anne-Edgar Wilke *Enumerating integral orbits of prehomogeneous representations*, since September 2019, supervised by K. Belabas.

PhD in progress: Sudarshan Shinde *Cryptographic applications of modular curves* since October 2016, supervised by R. Barbulescu with Pierre-Vincent Koseleff (Sorbonne Université).

8.2.3. Juries

X. Caruso has written a report for the doctoral dissertation by Léo Poyeton, ÉNS de Lyon: *Extensions de Lie p-adiques et (φ, Γ)-modules*.

X. Caruso has written a report for the doctoral dissertation by Christopher Doris, University of Bristol: *Aspects of p-adic computation*.

X. Caruso has written a report for the doctoral dissertation by Joelle Saade, Université de Limoges: *Méthodes symboliques pour les systèmes différentiels linéaires à singularité irrégulière*.

R. Barbulescu was part of the three members jury of the oral examination in mathematics for math-info the admission examination for ENS de Lyon

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

8.3. Popularization

8.3.1. Education

Alkindi : R. Barbulescu is one of the three organizers of the Alkindi contest, a contest for 13-to-15 year old students which gathers more than 60000 participants from France and Switzerland. D. Robert and the other members invite the winners of the Bordeaux region for a 2 hour visit each year.

8.3.2. Interventions

- from 27/05/2019 to 31/05/2019, X. Caruso supervised a stage at the fablab Coh@bit (at IUT Gradignan) to build some educational material
- 30/06/2019, X. Caruso: *Ramène pas ta science* on a physical experiment demonstrating that the fastest path between two points is an arc of cycloid
- 8-10/10/2019, A. Page: *Fête de la Science* at Inria Bordeaux, activity on cryptography (8 groups of students).
- 17/10/2019, X. Caruso and A. Page: *Village des 80 ans du CNRS*, discussion stand "Quizz des idées reçues" on research in mathematics.
- 19/10/2019, X. Caruso and M.-L. Chabanol: *Village des 80 ans du CNRS* on physical experiment demonstrating that the fastest path between two points is an arc of cycloid
- from 07/04/2019 to 14/04/2019, R. Barbulescu was one of two teachers for a math camp in Kinshasa of 150 students https://www.cnrs.fr/insmi/spip.php?article3190.
- from 06/07/2019 to 13/07/2019, R. Barbulescu was the main organiser for a math training camp which gathered the national teams for the International Olympiad of Mathematics of France, Romania and Bulgaria.
- 5/12/2019, D. Robert: small presentations of cryptography for the student of Ecole Normale Superieure de Lyon.

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° 1, pp. 173–210, http://projecteuclid.org/euclid.dmj/1272480934

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

[4] X. CARUSO, D. ROE, T. VACCON. *Tracking p-adic precision*, in "LMS J. Comput. Math.", 2014, vol. 17, pp. 274–294

[5] G. CASTAGNOS, F. LAGUILLAUMIE, I. TUCKER. *Practical Fully Secure Unrestricted Inner Product Functional Encryption modulo p*, in "Advances in Cryptology – ASIACRYPT 2018, Part II", T. PEYRIN, S. GALBRAITH (editors), Lecture Notes in Computer Science, International Association for Cryptologic Research, 2018, vol. 11273, pp. 733–764

[6] H. COHEN, F. STRÖMBERG. *Modular Forms: A Classical Approach*, Graduate Studies in Mathematics, American Mathematical Society, 2017, vol. 179, http://bookstore.ams.org/gsm-179/

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

[8] 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

[9] A. ENGE, W. HART, F. JOHANSSON. *Short addition sequences for theta functions*, in "Journal of Integer Sequences", 2018, vol. 18, n° 2, pp. 1–34

[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] G. CASTAGNOS. *Cryptography based on quadratic fields: cryptanalyses, primitives and protocols*, Université de Bordeaux, November 2019, Habilitation à diriger des recherches, https://tel.archives-ouvertes.fr/tel-02403707

Articles in International Peer-Reviewed Journals

[12] R. BARBULESCU, J. RAY. *Numerical verification of the Cohen-Lenstra-Martinet heuristics and of Greenberg's p-rationality conjecture*, in "Journal de Théorie des Nombres de Bordeaux", 2019, forthcoming, https://hal.archives-ouvertes.fr/hal-01534050

[13] A. BARTEL, A. PAGE. *Group representations in the homology of 3-manifolds*, in "Commentarii Mathematici Helvetici", March 2019, https://arxiv.org/abs/1605.04866 [*DOI :* 10.4171/CMH/455], https://hal.inria.fr/hal-01671748

[14] K. BELABAS, D. BERNARDI, B. PERRIN-RIOU. *La constante de Manin et le degré modulaire d'une courbe elliptique*, in "Publications Mathématiques de Besançon : Algèbre et Théorie des Nombres", 2019, n° 2, pp. 81-103, https://hal.archives-ouvertes.fr/hal-01766202

[15] J.-P. CERRI, P. LEZOWSKI. *Computation of Euclidean minima in totally definite quaternion fields*, in "International Journal of Number Theory", 2019, vol. 15, n° 1, pp. 43–66, https://hal.archives-ouvertes.fr/hal-01447059

[16] S. IONICA, E. THOMÉ. *Isogeny graphs with maximal real multiplication*, in "Journal of Number Theory", February 2020, vol. 207, pp. 385-422, https://arxiv.org/abs/1407.6672 [*DOI :* 10.1016/J.JNT.2019.06.019], https://hal.archives-ouvertes.fr/hal-00967742

[17] F. JOHANSSON, I. V. BLAGOUCHINE. *Computing Stieltjes constants using complex integration*, in "Mathematics of Computation", 2019, vol. 88, n° 318, https://arxiv.org/abs/1804.01679 , https://hal.inria.fr/hal-01758620

[18] A. RIFFAUT. *Equations with powers of singular moduli*, in "International Journal of Number Theory", 2019, vol. 15, n° 3, pp. 445-468 [*DOI :* 10.1142/S1793042119500234], https://hal.archives-ouvertes.fr/hal-01630363

International Conferences with Proceedings

[19] X. CARUSO, T. VACCON, T. VERRON. *Gröbner bases over Tate algebras*, in "ISSAC", Beijing, China, July 2019, https://arxiv.org/abs/1901.09574 [*DOI :* 10.1145/3326229.3326257], https://hal.archives-ouvertes.fr/hal-01995881

[20] G. CASTAGNOS, D. CATALANO, F. LAGUILLAUMIE, F. SAVASTA, I. TUCKER. *Two-Party ECDSA from Hash Proof Systems and Efficient Instantiations*, in "CRYPTO 2019 - 39th Annual International Cryptology Conference", Santa Barbara, United States, Advances in Cryptology – CRYPTO 2019, August 2019, vol. LNCS, n° 11694, pp. 191-221 [*DOI :* 10.1007/978-3-030-26954-8_7], https://hal.archives-ouvertes.fr/hal-02281931

[21] *Best Paper*
F. JOHANSSON. *Faster arbitrary-precision dot product and matrix multiplication*, in "26th IEEE Symposium on Computer Arithmetic (ARITH26)", Kyoto, Japan, June 2019, https://arxiv.org/abs/1901.04289 , https://hal.inria.fr/hal-01980399.

Scientific Books (or Scientific Book chapters)

[22] X. CARUSO. *An introduction to p-adic period rings*, in "An introduction to p-adic Hodge theory", 2019, https://arxiv.org/abs/1908.08424 , forthcoming, https://hal.archives-ouvertes.fr/hal-02268787

[23] H. COHEN. *An Introduction to Modular Forms*, in "Notes from the International School on Computational Number Theory", I. INAM, E. BÜYÜKAŞIK (editors), Tutorials, Schools, and Workshops in the Mathematical Sciences, Birkhäuser, 2019, pp. 3-62, https://arxiv.org/abs/1809.10907 , https://hal.inria.fr/hal-01883058

[24] H. COHEN. *Computational Number Theory in Relation with L-Functions*, in "Notes from the International School on Computational Number Theory", I. INAM, E. BÜYÜKAŞIK (editors), Tutorials, Schools, and

Workshops in the Mathematical Sciences, Birkhäuser, 2019, pp. 171-266, https://arxiv.org/abs/1809.10904 [*DOI :* 10.1007/978-3-030-12558-5_3], https://hal.inria.fr/hal-01883052

[25] H. COHEN. *Expansions at Cusps and Petersson Products in Pari/GP*, in "Elliptic Integrals, Elliptic Functions and Modular Forms in Quantum Field Theory", J. BLÜMLEIN, C. SCHNEIDER, P. PAULE (editors), Texts & Monographs in Symbolic Computation, Springer, 2019, https://arxiv.org/abs/1809.10908 , https://hal.inria.fr/hal-01883070

[26] F. JOHANSSON. *Numerical Evaluation of Elliptic Functions, Elliptic Integrals and Modular Forms*, in "Elliptic Integrals, Elliptic Functions and Modular Forms in Quantum Field Theory", J. BLÜMLEIN, C. SCHNEIDER, P. PAULE (editors), Texts & Monographs in Symbolic Computation, Springer, 2019, pp. 269-293, https://arxiv.org/abs/1806.06725 , https://hal.inria.fr/hal-01817952

Other Publications

[27] R. BARBULESCU, N. EL MRABET, L. GHAMMAM. *A taxonomy of pairings, their security, their complexity*, May 2019, working paper or preprint, https://hal.archives-ouvertes.fr/hal-02129868

[28] R. BARBULESCU, S. SHINDE. *A classification of ECM-friendly families using modular curves*, February 2019, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01822144

[29] X. CARUSO. *Residues of skew rational functions and linearized Goppa codes*, August 2019, https://arxiv.org/abs/1908.08430 - working paper or preprint, https://hal.archives-ouvertes.fr/hal-02268790

[30] J.-M. COUVEIGNES. *Enumerating number fields*, November 2019, https://arxiv.org/abs/1907.13617 - working paper or preprint, https://hal.archives-ouvertes.fr/hal-02375397

[31] J. KIEFFER. *Degree and height estimates for modular equations on PEL Shimura varieties*, January 2020, https://arxiv.org/abs/2001.04138 - working paper or preprint, https://hal.archives-ouvertes.fr/hal-02436057

[32] J. KIEFFER, A. PAGE, D. ROBERT. *Computing isogenies from modular equations between Jacobians of genus 2 curves*, January 2020, https://arxiv.org/abs/2001.04137 - working paper or preprint, https://hal.archives-ouvertes.fr/hal-02436133

[33] C. MAIRE, A. PAGE. *Codes from unit groups of division algebras over number fields*, 2019, https://arxiv.org/abs/1804.07108 - working paper or preprint, https://hal.inria.fr/hal-01770396

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

[35] E. MILIO, D. ROBERT. *Modular polynomials on Hilbert surfaces*, June 2019, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01520262

References in notes

[36] 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

[37] 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

[38] 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/