IN PARTNERSHIP WITH:
CNRS

Université de Bordeaux

Activity Report 2017

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
B9.4.2. - Mathematics

1. Personnel

Research Scientists

Andreas Enge [Team leader, Inria, Senior Researcher, HDR]
Fredrik Johansson [Inria, Researcher]
Aurel Page [Inria, Researcher, from Sep 2017]
Damien Robert [Inria, Researcher]

Faculty Members

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

PhD Students

Jared Guissmo Asuncion [Univ de Bordeaux, from Oct 2017]
Chloë Martindale [Universities Leiden and Bordeaux]
Emmanouil Tzortzakis [Universities Leiden and Bordeaux]

Technical staff

Jared Guissmo Asuncion [Inria, until Jun 2017]
Bill Allombert [CNRS]

Administrative Assistants

Anne-Laure Gautier [Inria]
Nathalie Robin [Inria]

Visiting Scientist

Abdoulaye Maiga [Univ. Dakar, Visiting Scientist]

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 SchÃÂ¶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 $n \geqslant 3$. 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 [24] for a recent account.

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

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

3.2. Function fields, algebraic curves and cryptology

Participants: Karim Belabas, Guilhem Castagnos, Jean-Marc Couveignes, Andreas Enge, Damien Robert, Emmanouil Tzortzakis.

Algebraic curves over finite fields are used to build the currently most competitive public key cryptosystems. Such a curve is given by a bivariate equation $\mathcal{C}(X, Y) = 0$ with coefficients in a finite field $\mathbb{F}_q$. The main classes of curves that are interesting from a cryptographic perspective are *elliptic curves* of equation $\mathcal{C} = Y^2 - (X^3 + aX + b)$ and *hyperelliptic curves* of equation $\mathcal{C} = Y^2 - (X^{2g+1} + \cdots)$ with $g \geqslant 2$.

The cryptosystem is implemented in an associated finite abelian group, the *Jacobian* $\mathrm{Jac}_\mathcal{C}$. Using the language of function fields exhibits a close analogy to the number fields discussed in the previous section. Let $\mathbb{F}_q(X)$ (the analogue of $\mathbb{Q}$) be the *rational function field* with subring $\mathbb{F}_q[X]$ (which is principal just as $\mathbb{Z}$). The *function field* of $\mathcal{C}$ is $K_\mathcal{C} = \mathbb{F}_q(X)[Y]/(\mathcal{C})$; it contains the *coordinate ring* $\mathcal{O}_\mathcal{C} = \mathbb{F}_q[X, Y]/(\mathcal{C})$. Definitions and properties carry over from the number field case $K/\mathbb{Q}$ to the function field extension $K_\mathcal{C}/\mathbb{F}_q(X)$. The Jacobian $\mathrm{Jac}_\mathcal{C}$ is the divisor class group of $K_\mathcal{C}$, which is an extension of (and for the curves used in cryptography usually equals) the ideal class group of $\mathcal{O}_\mathcal{C}$.

The size of the Jacobian group, the main security parameter of the cryptosystem, is given by an L-function. The GRH for function fields, which has been proved by Weil, yields the Hasse–Weil bound $(\sqrt{q}-1)^{2g} \leqslant |\operatorname{Jac}_{\mathcal{C}}| \leqslant (\sqrt{q}+1)^{2g}$, or $|\operatorname{Jac}_{\mathcal{C}}| \approx q^g$, where the *genus* g is an invariant of the curve that correlates with the degree of its equation. For instance, the genus of an elliptic curve is 1, that of a hyperelliptic one is $\frac{\deg_X \mathcal{C}-1}{2}$. An important algorithmic question is to compute the exact cardinality of the Jacobian.

The security of the cryptosystem requires more precisely that the *discrete logarithm problem* (DLP) be difficult in the underlying group; that is, given elements D_1 and $D_2 = xD_1$ of $\operatorname{Jac}_{\mathcal{C}}$, it must be difficult to determine x. Computing x corresponds in fact to computing $\operatorname{Jac}_{\mathcal{C}}$ explicitly with an isomorphism to an abstract product of finite cyclic groups; in this sense, the DLP amounts to computing the class group in the function field setting.

For any integer n, the *Weil pairing* e_n on $\mathcal{C}$ is a function that takes as input two elements of order n of $\operatorname{Jac}_{\mathcal{C}}$ and maps them into the multiplicative group of a finite field extension $\mathbb{F}_{q^k}$ with $k = k(n)$ depending on n. It is bilinear in both its arguments, which allows to transport the DLP from a curve into a finite field, where it is potentially easier to solve. The *Tate-Lichtenbaum pairing*, that is more difficult to define, but more efficient to implement, has similar properties. From a constructive point of view, the last few years have seen a wealth of cryptosystems with attractive novel properties relying on pairings.

For a random curve, the parameter k usually becomes so big that the result of a pairing cannot even be output any more. One of the major algorithmic problems related to pairings is thus the construction of curves with a given, smallish k.

3.3. Complex multiplication

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

Complex multiplication provides a link between number fields and algebraic curves; for a concise introduction in the elliptic curve case, see [26], for more background material, [25]. In fact, for most curves $\mathcal{C}$ over a finite field, the endomorphism ring of $\operatorname{Jac}_{\mathcal{C}}$, which determines its L-function and thus its cardinality, is an order in a special kind of number field K, called *CM field*. The CM field of an elliptic curve is an imaginary-quadratic field $\mathbb{Q}(\sqrt{D})$ with $D < 0$, that of a hyperelliptic curve of genus g is an imaginary-quadratic extension of a totally real number field of degree g. Deuring's lifting theorem ensures that $\mathcal{C}$ is the reduction modulo some prime of a curve with the same endomorphism ring, but defined over the *Hilbert class field* H_K of K.

Algebraically, H_K is defined as the maximal unramified abelian extension of K; the Galois group of H_K/K is then precisely the class group Cl_K. A number field extension H/K is called *Galois* if $H \simeq K[X]/(f)$ and H contains all complex roots of f. For instance, $\mathbb{Q}(\sqrt{2})$ is Galois since it contains not only $\sqrt{2}$, but also the second root $-\sqrt{2}$ of X^2-2, whereas $\mathbb{Q}(\sqrt[3]{2})$ is not Galois, since it does not contain the root $e^{2\pi i/3}\sqrt[3]{2}$ of X^3-2. The *Galois group* $\operatorname{Gal}_{H/K}$ is the group of automorphisms of H that fix K; it permutes the roots of f. Finally, an *abelian* extension is a Galois extension with abelian Galois group.

Analytically, in the elliptic case H_K may be obtained by adjoining to K the *singular value* $j(\tau)$ for a complex valued, so-called *modular* function j in some $\tau \in \mathcal{O}_K$; the correspondence between $\operatorname{Gal}_{H/K}$ and Cl_K allows to obtain the different roots of the minimal polynomial f of $j(\tau)$ and finally f itself. A similar, more involved construction can be used for hyperelliptic curves. This direct application of complex multiplication yields algebraic curves whose L-functions are known beforehand; in particular, it is the only possible way of obtaining ordinary curves for pairing-based cryptosystems.

The same theory can be used to develop algorithms that, given an arbitrary curve over a finite field, compute its L-function.

A generalisation is provided by *ray class fields*; these are still abelian, but allow for some well-controlled ramification. The tools for explicitly constructing such class fields are similar to those used for Hilbert class fields.

4. Highlights of the Year

4.1. Highlights of the Year

Aurel Page has been recruited as a Inria CR in the team.

Damien Robert organised a one-week workshop with the members of the associated team FAST with several African countries.

The book [18] by Henri Cohen on *Modular Forms: A Classical Approach* has been published.

4.1.1. Awards

The paper [11] describing Arb in the IEEE Transactions on Computers was selected as the best paper of this journal's Special Issue on Computer Arithmetic.

BEST PAPER AWARD:

[11]
F. JOHANSSON. *Arb: Efficient Arbitrary-Precision Midpoint-Radius Interval Arithmetic*, in "IEEE Transactions on Computers", August 2017, vol. 66, n^{o} 8, pp. 1281 - 1292 [*DOI :* 10.1109/TC.2017.2690633], https://hal.inria.fr/hal-01678734

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. 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: Damien Robert, Gaëtan Bisson and Romain Cosset
- Contact: Gaëtan Bisson
- 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/

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

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-bordeaux1.fr/~belabas/research/software/cubic-1.2.tgz

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

5.7. 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

5.8. 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/

5.10. PARI/GP

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

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

6. New Results

6.1. Non commutative number theory

Participant: Jean Paul Cerri.

Pierre Lezowski has studied in [12], Euclidean properties of matrix algebras. He proved that if A is a commutative ring and if $n > 1$ is an integer , then $M_n(A)$ is right and left Euclidean if and only if A is a principal ideal ring. Moreover, under the hypothesis that the stathm takes integer values, he established that if A is an integral domain, then $M_n(A)$ is ω-stage right and left Euclidean if and only if A is a Bézout ring. He also proved, under the same hypothesis, that if A is a K-Hermite ring, then $M_n(A)$ is $(4n-3)$-stage left and right Euclidean, that if A is an elementary divisor ring, then $M_n(A)$ is $(2n-1)$-stage left and right Euclidean, and that if A is a principal ideal ring, then $M_n(A)$ is 2-stage right and left Euclidean. In each case, he obtained an explicit algorithm allowing to compute, among other things, right or left gcd in $M_n(A)$.

Jean-Paul Cerri and Pierre Lezowski have generalized in [19], Cerri's algorithm (for the computation of the upper part of the norm-Euclidean spectrum of a number field) to totally definite quaternion fields. This allowed them to establish the exact value of the norm-Euclidean minimum of many orders in totally definite quaternion fields over a quadratic number field. Before this work, nobody knew how to compute the exact value of such a minimum when the base number field has degree > 1. They also proved that the Euclidean minimum and the inhomogeneous minimum of orders in such quaternion fields are always equal and that moreover they are rational under the hypothesis that the base number field is not quadratic, which remains the only open case, as for real number fields.

In [13] Lezowski determines which cyclic field of degree d are norm-Euclidean for
$d = 5, 7, 19, 31, 37, 43, 47, 59, 67, 71, 73, 79, 97$.

6.2. Cryptographic Protocols

Participant: Guilhem Castagnos.

In [16] G. Castagnos, L. Imbert, and F. Laguillaumie revisit a recent cryptographic primitive called *encryption switching protocols* (ESP). This primitive was introduced by Couteau, Peters and Pointcheval last year. It allows to switch ciphertexts between two encryption schemes. If such an ESP is built with two schemes that are respectively additively and multiplicatively homomorphic, it naturally gives rise to a secure 2-party computation protocol. It is thus perfectly suited for evaluating functions, such as multivariate polynomials, given as arithmetic circuits. Couteau et al. built an ESP to switch between Elgamal and Paillier encryptions which do not naturally fit well together. Consequently, they had to design a clever variant of Elgamal over $\mathbf{Z}/n\mathbf{Z}$ with a costly shared decryption.

In this work, Castagnos *et. al.* first present a conceptually simple generic construction for encryption switching protocols. Then, they give an efficient instantiation of our generic approach that uses two well-suited protocols, namely a variant of Elgamal in $\mathbf{Z}/p\mathbf{Z}$ and the Castagnos-Laguillaumie encryption which is additively homomorphic over $\mathbf{Z}/p\mathbf{Z}$. Among other advantages, this allows to perform all computations modulo a prime p instead of an RSA modulus. Overall, this solution leads to significant reductions in the number of rounds as well as the number of bits exchanged by the parties during the interactive protocols. They also show how to extend its security to the malicious setting.

This paper was presented at the CRYPTO Conference 2017, and is part of the ALAMBIC project.

6.3. Algorithmic number theory

Participant: Henri Cohen.

The book [18] by Henri Cohen on *Modular Forms: A Classical Approach* has been published. The theory of modular forms is a fundamental tool used in many areas of mathematics and physics. It is also a very concrete subject in itself and abounds with an amazing number of surprising identities. This comprehensive textbook, gives a complete picture of the classical aspects of the subject, with an emphasis on explicit formulas. Content include: elliptic functions and theta functions, the modular group, its subgroups, and general aspects of holomorphic and nonholomorphic modular forms, with an emphasis on explicit examples. The heart of the book is the classical theory developed by Hecke and continued up to the Atkin–Lehner–Li theory of newforms and including the theory of Eisenstein series, Rankin–Selberg theory, and a more general theory of theta series including the Weil representation. The final chapter also explores in some detail more general types of modular forms such as half-integral weight, Hilbert, Jacobi, Maass, and Siegel modular forms.

The article by Bill Allombert, Jean-Paul Allouche and Michel Mendès France on *Euler's divergent series and an elementary model in Statistical Physics* has been published in Statistical Physics Ars Mathematica Contemporanea. This article study the multiple integral of a multivariate exponential taken with respect either to the Lebesgue measure or to the discrete uniform Bernoulli measure. In the first case the integral is linked to Euler's everywhere divergent power series and its generalizations, while in the second case the integral is linked to a one-dimensional model of spin systems as encountered in physics.

Bill Allombert has worked with Nicolas Brisebarre and Alain Lasjaunias on *a two-valued sequence and related continued fractions in power series fields*. They explicitly describe a noteworthy transcendental continued fraction in the field of power series over $\mathbb{Q}$, having irrationality measure equal to 3. This continued fraction is a generating function of a particular sequence in the set $\{1, 2\}$.

In the Pari software, K. Belabas and H. Cohen have added an extensive new package `mf` for modular forms. This package allows to build spaces of classical modular form $M_k(\Gamma_0(N), \chi)$ where $2k \in \mathbb{Z}$ and perform standard tasks like finding bases, splitting the space using Hecke operators and the computation of eigenforms. It also solves important difficult problems: the computation of forms of weight 1, the realization of Shimura lifts as an explicit isomorphism between Kohnen's $+$-space $S_k^+(\Gamma 0(4N), \chi)$ and $S_{2k-1}(\Gamma_0(N), \chi^2)$ and the Fourier expansion of $f \mid_k \gamma$ for arbitrary f and arbitrary $\gamma \in \mathrm{GL}_2(\mathbb{Q})^+$, which includes as a special case the expansion of f at all cusps (where other modular form packages usualy deal with the expansion at infinity and the cusps reachable via Atkin-Lehner operators, e.g. all cusps in squarefree levels). The latter is especially important as it allows an explicit description of Atkin-Lehner operators, the evaluation of f arbitrary points in the upper-half plane, the computation of period polynomials and Pettersson products, etc.

6.4. Elliptic curve and Abelian varieties cryptology

Participant: Damien Robert.

In [22], E. Milio and D. Robert describe an algorithm to evaluate in quasi-linear time Hilbert modular functions in dimension 2, and also how to recover in time quasi-linear the period matrix from the value of the function. They apply this theory to the modular functions $j(\tau/\beta)$ and $\theta(\tau/\beta)$ where β is a totally real positive number of the quadratic real field corresponding to the Hilbert surface to construct modular polynomials parametrizing cyclic isogenies between principally polarised abelian varieties. This extends the construction of classical modular polynomials but allow to have much smaller polynomials, which allow to compute them up to norm $\ell = 91$ rather than $\ell = 7$ in dimension 2 for classical polynomials.

In [20], Dudeanu, Alina and Jetchev, Dimitar and Robert, Damien and Vuille, Marius describe an algorithm to compute cyclic isogenies from their kernels. This extends the work of [10] from isogenies with maximal isotropic kernels for the Weil pairing to cyclic isogenies, using real multiplication. Such isogenies are indispensable to fully explore the isogeny graph and will be able to speed up a lot of algorithms that needs isogenous curves, like the CRT method for class polynomials.

6.5. Arbitrary-precision ball arithmetic

Participant: Fredrik Johansson.

During the year, F. Johansson has released three new versions (2.10, 2.11 and 2.12) of the Arb software for arbitrary-precision ball arithmetic.

The paper [11] describing Arb has been published in the IEEE Transactions on Computers and was selected as the best paper of this journal's Special Issue on Computer Arithmetic. As a result, a video presentation was featured on the journal's website and Johansson was invited to present the paper in a special session at the 24th IEEE Symposium on Computer Arithmetic (ARITH24) at Imperial College London, UK.

In [21], Johansson describes the first complete algorithm for computing the Lambert W function rigorously in complex ball arithmetic.

6.6. Python and Julia computer algebra packages

Participant: Fredrik Johansson.

F. Johansson together with C. Fieker, W. Hart and T. Hofmann of TU Kaiserslautern have developed Nemo and Hecke, two packages for computer algebra and algebraic number theory using the Julia programming language. The paper [17] describing Nemo and Hecke has been published in the proceedings of ISSAC, the main international computer algebra conference.

The paper [15] describing the SymPy package for computer algebra in Python has been published. SymPy is a highly collaborative international project and F. Johansson is one of the 27 coauthors of this paper. Johansson's main contributions to the software include developing the mpmath package used for arbitrary-precision numerical evaluation. In addition, Johansson has issued the stable version 1.0 release of mpmath.

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.

7.2. European Initiatives

7.2.1. FP7 & H2020 Projects

Title: OpenDreamKit

Program: H2020

Duration: January 2016 - December 2020

Coordinator: Nicolas Thiéry

Inria contact: Karim Belabas

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

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

7.3. International Initiatives

7.3.1. Inria International Labs

7.3.1.1. FAST

Title: (Harder Better) FAster STronger cryptography

International Partner

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

Start year: 2017

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

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

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

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

7.3.2. Inria International Partners

7.3.2.1. Informal International Partners

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

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

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Researchers visiting the team to give a talk to the team seminar include Damien Stehlé (ENS Lyon), Cécile Pierrot (Centrum Wiskunde and Informatica, Amsterdam), Christophe Petit (Oxford), Benjamin Wesolowski (EPFL), Bernhard Schmidt (Nanyang Technological University, Singapore), Mohamadou Sall (Université Cheikh Anta Diop, Dakar, Sénégal), Emmanuel Fouotsa (The University of Bamenda, Cameroon), Abdoulaye Maiga (Université Cheikh Anta Diop, Dakar, Sénégal), Tony Ezome (Université des Sciences et Techniques de Masuku (USTM), Franceville, Gabon), Abdoul Aziz Ciss (Université Cheikh Anta Diop, Dakar, Sénégal), José Manuel Rodriguez Caballero (Labri), Jean Kieffer (ENS Paris), Christian Klein (Institut de Mathématiques de Bourgogne), Frank Vallentin (Mathematisches Institut, Universität zu Köln).

7.4.2. *Visits to International Teams*

Jared Asuncion went to the Autumn school: Topics in arithmetic and algebraic geometry last 9 - 13 October 2017 at the University of Mainz in Mainz, Germany.

Jared Asuncion went to see his cosupervisor, Marco String last 6 - 10 November 2017 at the Universiteit Leiden in Leiden, The Netherlands. It is planned to stay in Leiden for a period of six months while working on his PhD.

Jared Asuncion went to the 21st Workshop on Elliptic Curve Cryptography last 13 - 15 November 2017 at the Radboud University in Nijmegen, The Netherlands.

A. Page visited C. Maire in Cornell University (Ithaca, US) from November 27th to December 4th and gave a research talk there on December 1st. He then visited Michael Lipnowski in the Institute for Advanced Studies (Princeton, US) from December 4th to December 14th.

A. Enge visited Bernhard Schmidt in Nanyang Technological University, Singapore for three weeks.

Fredrik Johansson participated in the OSCAR: Antic workshop at TU Kaiserslautern, Germany and gave an invited talk on "Fundamental algorithms in Arb".

Fredrik Johansson participated in the workshop on Elliptic Integrals, Elliptic Functions and Modular Forms in Quantum Field Theory at DESY, Zeuthen, Germany, and gave an invited talk on "Numerics of classical elliptic functions, elliptic integrals and modular forms".

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. *Scientific Events Organisation*

8.1.1.1. General Chair, Scientific Chair

B. Allombert and K. Belabas organized a workshop PARI/GPin Lyon on 09-13 January 2017.

B. Allombert and K. Belabas organized a workshop “Elliptic curves, modular forms and L-functions in the PARI/GPsystem” in Clermont-Ferrand on 19-23 June 2017.

B. Allombert and A. Page organized a mini-workshop PARI/GPin Oujda, Morocco on 22-23 November 2017.

8.1.2. *Journal*

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

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

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

8.1.3. *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.

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

8.1.4. Research Administration

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

Since January 2015, K. Belabas is vice-head of the Math Institute (IMB). He also leads the computer science support service (“cellule informatique”) of IMB and coordinates the participation of the institute in the regional computation cluster PlaFRIM.

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

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

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

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

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

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

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

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

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

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

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

Licence : Jean-Paul Cerri, Algèbre bilinéaire et géométrie, 35h TD, L3, Université de Bordeaux, France

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

Master : Jean-Paul Cerri, Cryptologie, 24h TD, M1, Université de Bordeaux, France

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

8.2.2. Supervision

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: Chloë Martindale, *Isogeny graphs*, since 2013, supervised by A. Enge and Marco Streng (Universiteit Leiden).

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

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

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

Master 2: Margarita Pierrakea, *Supersingular isogeny key-exchange*, supervised by D. Robert.

8.2.3. Juries

- A. Enge has written a report for the doctoral dissertation by Alexandre Le Meur, Université de Rennes, sur *Formules de Thomae généralisées à des courbes galoisiennes résolubles sur la droite projective*.
- A. Enge has written a report for the doctoral dissertation by Alexandre Gélin, Université Pierre et Marie Curie, *Class Group Computations in Number Fields and Applications to Cryptology*. K. Belabas was a member of the defense committee.
- K. Belabas has written a report for the doctoral dissertation of Thomas Camus, Université Grenoble-Alpes, *Méthodes algorithmiques pour les réseaux algébriques*.
- K. Belabas was a member of the defense committee of José Villanueva-Guttierez, Université de Bordeaux, *Sur quelques questions en théorie d'Iwasawa*.
- K. Belabas was a member of the defense committee of Philippe Moustrou, Université de Bordeaux, *Geometric distance graphs, lattices and polytopes*.
- J-M. Couveignes was a member of the defense committee of Carine Jaber (advisor Christian Klein), Université de Dijon, *Approche algorithmique au domaine fondamental de Siegel* the 28 June 2017.
- J-M. Couveignes was the president of the defense committee of Matthieu Rambaud (advisor Hugues Randriambololona), Telecom-ParisTech, *Shimura curves and bilinear multiplication algorithms in finite fields* the 2 September 2017.
- D. Robert is a member of the jury of Agregations de Mathematiques. He is also the codirector with Alain Couvreur of the option “calcul formel” of the Modelisation part of the oral examination.

8.3. Popularization

The book Guide to Pairing-Based Cryptography [27] has been published by CHAPMAN and HALL/CRC. D. Robert wrote with Sorina Ionica the chapter “Pairings” of this book. This book aims to help Engineers understand and implement pairing based cryptography; in the Chapter “Pairings”, D. Robert give a self contained definition and proof of the Weil and Tate pairing; including how to handle divisors with non disjoint support (this is often skipped in scientific papers but is important for practical implementations).

A. Page gave a popularization talk “À la découverte de la cryptologie : la science du secret” during the Fête de la Science event. Two groups of high school students and one group of Inria agents participated in this activity. Following this talk, three high school students decided to work on the RSA cryptosystem for their TPE essay and came back to the IMB to meet A. Page and talk about this topic in greater detail.

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^{o} 1, pp. 24–41

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

Publications of the year

Articles in International Peer-Reviewed Journals

[11] *Best Paper*
F. Johansson. *Arb: Efficient Arbitrary-Precision Midpoint-Radius Interval Arithmetic*, in "IEEE Transactions on Computers", August 2017, vol. 66, n^{o} 8, pp. 1281 - 1292 [*DOI :* 10.1109/TC.2017.2690633], https://hal.inria.fr/hal-01678734.

[12] P. Lezowski. *On some Euclidean properties of matrix algebras*, in "Journal of Algebra", September 2017, vol. 486, pp. 157–203, 38 pages, some minor corrections. [*DOI :* 10.1016/j.jalgebra.2017.05.018], https://hal.archives-ouvertes.fr/hal-01135202

[13] P. Lezowski, K. J. McGown. *The Euclidean algorithm in quintic and septic cyclic fields*, in "Mathematics of Computation", September 2017, vol. 86, n^{o} 307, pp. 2535–2549, https://arxiv.org/abs/1601.03433 - 15 pages, some corrections and improvements, especially in the proof of Proposition 6.1 [*DOI :* 10.1090/mcom/3169], https://hal.archives-ouvertes.fr/hal-01258906

[14] N. Mascot. *Certification of modular Galois representations*, in "Mathematics of Computation", 2017, https://arxiv.org/abs/1312.6418 , https://hal.archives-ouvertes.fr/hal-01426832

Articles in Non Peer-Reviewed Journals

[15] A. MEURER, C. SMITH, M. PAPROCKI, O. ČERTÍK, S. KIRPICHEV, M. ROCKLIN, A. KUMAR, S. IVANOV, J. MOORE, S. SINGH, T. RATHNAYAKE, S. VIG, B. GRANGER, R. MULLER, F. BONAZZI, H. GUPTA, S. VATS, F. JOHANSSON, F. PEDREGOSA, M. CURRY, A. TERREL, Š. ROUČKA, A. SABOO, I. FERNANDO, S. KULAL, R. CIMRMAN, A. SCOPATZ. *SymPy: symbolic computing in Python*, in "PeerJ Comput.Sci.", 2017, vol. 3, e103 p. [*DOI :* 10.7717/PEERJ-CS.103], https://hal.archives-ouvertes.fr/hal-01645958

International Conferences with Proceedings

[16] G. CASTAGNOS, L. IMBERT, F. LAGUILLAUMIE. *Encryption Switching Protocols Revisited: Switching Modulo p*, in "CRYPTO 2017 - 37th International Cryptology Conference", Santa Barbara, United States, Advances in Cryptology – CRYPTO 2017, August 2017, vol. 10401, pp. 255-287 [*DOI :* 10.1007/978-3-319-63688-7_9], https://hal-lirmm.ccsd.cnrs.fr/lirmm-01587451

[17] C. FIEKER, W. HART, T. HOFMANN, F. JOHANSSON. *Nemo/Hecke: Computer Algebra and Number Theory Packages for the Julia Programming Language*, in "ISSAC '17", Kaiserslautern, Germany, July 2017 [*DOI :* 10.1145/3087604.3087611], https://hal.inria.fr/hal-01524140

Scientific Books (or Scientific Book chapters)

[18] H. COHEN, F. STRÖMBERG. *Modular Forms: A Classical Approach*, Graduate Studies in Mathematics, American Mathematical Society, 2017, vol. 179, 700 p. , https://hal.inria.fr/hal-01677348

Other Publications

[19] J.-P. CERRI, P. LEZOWSKI. *Computation of Euclidean minima in totally definite quaternion fields*, March 2017, 22 pages, some improvements and corrections, especially in Sections 4 and 5., https://hal.archives-ouvertes.fr/hal-01447059

[20] A. DUDEANU, D. JETCHEV, D. ROBERT, M. VUILLE. *Cyclic Isogenies for Abelian Varieties with Real Multiplication*, November 2017, working paper or preprint, https://hal.inria.fr/hal-01629829

[21] F. JOHANSSON. *Computing the Lambert W function in arbitrary-precision complex interval arithmetic*, May 2017, working paper or preprint, https://hal.inria.fr/hal-01519823

[22] E. MILIO, D. ROBERT. *Modular polynomials on Hilbert surfaces*, September 2017, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01520262

[23] A. PAGE, A. BARTEL. *Group representations in the homology of 3-manifolds*, December 2017, working paper or preprint, https://hal.inria.fr/hal-01671748

References in notes

[24] 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

[25] 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

[26] 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/

[27] S. IONICA, D. ROBERT. *Pairings*, MIS, 2016, CRC Press, to appear, https://hal.archives-ouvertes.fr/hal-01323882