INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team CACAO

Curves, Algebra, Computer Arithmetic, and so On

Nancy - Grand Est

THEME SYM

Table of contents

1. Team

Head of project-team
Guillaume Hanrot [research director, INRIA, HdR]

Vice-head of project-team
Paul Zimmermann [research director, INRIA, HdR]

Administrative assistant
Emmanuelle Deschamps

Research scientists
Pierrick Gaudry [research scientist, CNRS]
Emmanuel Thomé [research scientist, INRIA]
Marion Videau [assistant professor, Université Henri Poincaré]

PhD. students
Thomas Houtmann [DGA grant, DGA, defense planned in 2008]
Alexander Kruppa [CNRS grant, defense planned in 2010]
Damien Robert [MESR grant, UHP, defense planned in 2010]

Technical staff
Philippe Théveny [ODL grant, INRIA, since Sept. 1st]

Post-doctoral fellow
Laurent Fousse [MESR grant, UHP, until Aug. 31st]
Nuno Franco [Auxiliar Professor, University of Evora, Portugal]

2. Overall Objectives

2.1. Overall Objectives

The CACAO project-team has been officially created on October 9, 2006, after having *de facto* existed for more than one year. The objectives of the project-team are along the following lines:

- Study arithmetic of curves of small genus, with a particular emphasis on applications to cryptology;
- Improve the efficiency and the reliability of arithmetics in a broad sense (i.e., the arithmetics of a wide variety of objects).

These two objectives interplay strongly. On the one hand, arithmetics are at the core of optimizing algorithms on curves, starting evidently with the arithmetic of curves themselves. On the other hand, curves can sometimes be a tool to solve some arithmetical problems as integer factorization.

To reach these objectives, we have isolated three key axes of work:

- **Algebraic Curves and Cryptology**: the main issue here is to investigate curves of small genus over finite fields (base field $\mathbb{F}_{p^n}$, for various p and n). The main tasks are to compute in the Jacobian of a given curve, to be able to check that this variety is suitable for cryptography (cardinality, smoothness test) and to solve problems in those structures (discrete logarithm). Applications go from number theory (integer factorization) to cryptography (an alternative to RSA).
- **Arithmetics**: Here, we consider algorithms dealing with multiple-precision integers, floating-points numbers, p-adic numbers and finite fields. For such basic data structures, we do not expect new algorithms with better asymptotic behavior to be discovered; however, since those are first-class objects in all our computations, any speedup is most welcome, even by a factor of 2. Since January 2007, CACAO has also been strongly involved in a project on the number field sieve (NFS), an integer factorization algorithm. We aim at developing an efficient implementation of the NFS, study its distribution, and fine-tune it in the currently "practical" range, i.e., 100-150 decimal digits.

- **Linear Algebra and Lattices**: solving large linear systems is a key point of factoring and of discrete logarithm algorithms, which we need to investigate if curves are to be applied in cryptology. Lattices are central points of the new ideas that have emerged over the very last years for several problems in computer arithmetic or discrete logarithms algorithms.

Another new direction of research has started since Fall 2006 with the arrival of Marion Videau, who has been hired as an assistant professor at UHP, coming from the CODES project-team (INRIA Paris - Rocquencourt). This should allow the project-team to start an axis around symmetric primitives for cryptology; this is an interesting complement to the expertise already present regarding asymmetric (and especially curve-based) primitives for cryptology.

3. Scientific Foundations

3.1. Scientific Foundations

3.1.1. Algebraic Curves and Cryptology

Though we are interested in algebraic curves by themselves, the applications to cryptology remain a motivation of our research, which is therefore especially focused on curves defined over finite fields.

In the mid-eighties, Koblitz [27] and Miller [29] proposed to use elliptic curves as a basis of public key cryptosystems. Indeed, the set of points on an elliptic curve is an abelian group, which is finite if the base field is a finite field. In this group, the discrete logarithm problem is thought to be difficult in general, in the sense that the best known algorithm to solve it has an exponential complexity. This has to be compared with the classical RSA algorithm, the security of which relies on the difficulty of factoring integers, but where the best known factoring algorithm has subexponential complexity. In practice, this means that the size of the parameters is much smaller for elliptic curve based cryptosystems than for classical ones.

More generally, for an algebraic curve over a finite field, there is a finite abelian group associated to it, called the Jacobian of the curve. Algebraic curves can be classified by their genus; the genus of a conic is zero and elliptic curves are curves of genus 1 (in that case, the Jacobian is isomorphic to the curve). As long as the genus is not too large, the discrete logarithm problem in the Jacobian of a curve is thought to be difficult in general, therefore one can also base cryptosystems on non-elliptic curves.

The main algorithmic tasks in relation to the use of curves in cryptography are the following:

1. Have an explicit description of the group and the group operation, as efficient as possible. The speed of ciphering and deciphering is indeed directly linked to the efficiency of the group operation.
2. Construct curves suitable for cryptographic use: the minimal requirement for the discrete logarithm to be difficult is to have a large prime factor in the group order. It is therefore necessary to compute the group order to check that property. This is what we call the *point counting task*.
3. Study the security of curve-based primitives. By this, since no general framework exists to assess that security, we mean undertake an as thorough as possible study of the security offered by those groups. The most standard way to do this is by trying to solve discrete logarithm problems in certain classes of curves.

3.1.2. Linear Algebra and Lattices

With “linear algebra and lattices”, we denote two classes of problems of interest: computing vectors of the kernel of a large sparse matrix defined over a finite field, and studying algorithms to handle lattices that are given by a vector basis.

Huge linear systems are frequently encountered as last steps of "index-calculus" based algorithms for factoring or discrete logarithm computations. Those systems correspond to a particular presentation of the underlying group by generators and relations; they are thus always defined on a base ring which is $\mathbb{Z}$ modulo the exponent of the group, typically $\mathbb{Z}/2\mathbb{Z}$ in the case of factorization, $\mathbb{Z}/(q^n-1)\mathbb{Z}$ when trying to solve a discrete logarithm problem over $\mathbb{F}_{q^n}^*$. Those systems are often extremely sparse, so that specialized algorithms (Lanczós, Wiedemann) relying only on the evaluation of matrix-vector products essentially have a quadratic complexity, instead of being cubic with the classical Gaussian elimination.

The sizes of the matrices that are handled in record computations are such that they do not fit in the central memory of a single machine, even using a representation adapted to their sparse nature. Some parallelism is then required, yielding various difficulties that are different from the ones encountered in the classical linear algebra problems linked to numerical analysis. Specifically, dealing with matrices defined over finite fields precludes direct adaptation of numerical methods based on the notion of convergence and fixed-point theorems.

The second main topic is algorithmic lattice theory. Lattices are key tools in numerous problems in computer algebra, algorithmic number theory and cryptology. The typical questions one wants to solve are to find the shortest nonzero vector in a lattice and to find the closest lattice vector to a given vector. A more general concern is to find a better lattice basis than the one provided by the user; by "better" we mean that it consists of short, almost orthogonal vectors. This is a difficult problem in general, since finding the shortest nonzero vector is already NP-hard, under probabilistic reductions. In 1982, Lenstra, Lenstra, and Lovász [28] defined the notion of a LLL-reduced basis and described an algorithm to compute such a basis in polynomial time. Although not always sufficient, the LLL-reduction is sometimes enough for the application. Some stronger notions of reduction exist, such as Hermite-Korkine-Zolotarev [24] (HKZ) reduction, which require exponential or super-exponential time but solve the shortest vector problem in an exact way. Schnorr [30] introduced a complete hierarchy of reductions ranging from LLL to HKZ both in quality and in complexity, the so-called k-BKZ reductions.

3.1.3. Arithmetics

We consider here the following arithmetics: integers, rational numbers, integers modulo a fixed modulus n, finite fields, floating-point numbers and p-adic numbers. We can divide those numbers in two classes: *exact numbers* (integers, rationals, modular computations or finite fields), and *inexact numbers* (floating-point and p-adic numbers).

Algorithms on integers (respectively floating-point numbers) are very similar to those on polynomials, respectively Taylor or Laurent series. The main objective in that domain is to find new algorithms that make operations on those numbers more efficient. These new algorithms may use an alternate number representation.

In the case of integers, we are interested in multiprecision arithmetic. Various algorithms are to be used, depending on the sizes of the objects, starting with the most simple "schoolbook" methods to the most advanced, asymptotically fast algorithms. The latter are often based on Fourier transforms.

The case of modular arithmetic and finite fields is the first where the representation of the elements has to be chosen carefully. Depending on the type of operations one wants to perform, one must choose between a classical representation, the Montgomery representation, a look-up table, a polynomial representation, a normal basis representation, ... Then appropriate algorithms must be chosen.

With p-adic numbers, we get the first examples of non-exact representations. In that setting, one has to keep track of the precision all along a computation. The mechanisms to handle that issue can vary: since the precision losses are not too difficult to control, one can work with a fixed global precision, or one can choose to have each element carrying its precision. Additionally, there are several choices for representing elements, in particular when dealing with algebraic extensions of the p-adics (ramified or unramified).

Last but not least, we are interested in the arithmetics of real numbers of floating-point type. Again, we have a notion of approximation. It is therefore necessary to decide of a *format* that defines a set of representable numbers. Then, when the result of an arithmetical operation on two representable numbers is not representable,

one should define a way to *round* it to a meaningful representable number. The purpose of the IEEE-754 standard is to give a uniform answer to these questions in order to guarantee the reliability and portability of floating-point computations. The standard is restricted to the 4 basic field operations and the square root on a small number of possible formats (single, double, double-extended binary formats), but it can be extended to arbitrary precision and all classical mathematical functions. This leads to efficiency questions, in particular to guarantee that the result of an operation has been correctly rounded.

4. Application Domains

4.1. Application Domains

4.1.1. Cryptology.

The main application domain of our project-team is cryptology. Algebraic curves have taken an increasing importance in cryptology over the last ten years. Various works have shown the usability and the usefulness of elliptic curves in cryptology, standards (for instance, IEEE P1363 [26] and real-world applications (like the electronic passport).

We study the suitability of higher genus curves to cryptography (mainly hyperelliptic curves of genus two, three). In particular, we work on improving the arithmetic of those curves, on the point counting problem, and on the discrete logarithm problem.

We also have connections to cryptology through the study and development of the integer LLL algorithm, which is one of the favourite tools to cryptanalyze public-key cryptosystems. Examples are the cryptanalysis of knapsack-based cryptosystems, the cryptanalyses of some fast variants of RSA, the cryptanalyses of fast variants of signature schemes such as DSA or Elgamal, or the attacks against lattice based cryptosystems like NTRU. The use of floating-point arithmetic dramatically speeds up this algorithm, which renders the aforementioned cryptanalyses more feasible.

Finally, we are studying integer factoring algorithms which are of utmost importance for the evaluation of the security of the still widely used RSA cryptosystem. In the context of our ANR CADO grant, we are investigating the Number Field Sieve algorithm, which is the best known algorithm for factoring numbers of the kind used in practical RSA instances.

4.1.2. Computational Number Theory Systems.

We have strong ties with several computational number theory systems, and code written by members of the project-team can be found in the Magma software and in the Pari/GP software.

Magma[1] is the leading computational number theory software. It also has some features of computer algebra (algebraic geometry, polynomial system solving) but not all of what is expected of a computer algebra system. It is developed by the team of John Cannon in Sydney.

Pari/GP[2] is a computational number theory system which comes with a library which can be used to access Pari functions within a C program. It has originally been developed at the Bordeaux 1 University, and is currently maintained (and expanded) by Karim Belabas, from Bordeaux University. It is free (GPL) software. We sometimes use it for validation of our algorithms. Again, some code written by members of the project-team is incorporated into Pari.

SAGE[3] is a new open-source computer algebra system. Its development was initiated by William Stein (Univ. of Washington, Seattle). Instead of reinventing the wheel, SAGE incorporates the most efficient open-source packages in each domain, for example SINGULAR, PARI/GP, NTL, LINBOX, and the software tools MPFR and GMP-ECM developed by CACAO. Although quite new, there is already a community of active developers around SAGE. This system might become a good alternative to Maple, Mathematica, and Magma to disseminate our research in the future.

[1] http://magma.maths.usyd.edu.au/magma/
[2] http://pari.math.u-bordeaux.fr
[3] http://sagemath.org

4.1.3. Arithmetics.

Another indirect transfer is the usage of MPFR in GFORTRAN (since 2004), and in GCC, up from version 4.3. MPFR is currently used at compile-time, to convert expressions like $\sin(3.1416)$ into binary double-precision, when the rounding mode can be statically determined. The MPFR library is also used by the CGAL software, a library for computational geometry developed by the Geometrica project-team (INRIA Sophia Antipolis - Méditerranée).

5. Software

5.1. Introduction

A major part of the research done in the CACAO project-team is published within software. On the one hand, this enables everyone to check that the algorithms we develop are really efficient in practice; on the other hand, this gives other researchers — and us of course — basic software components on which they — and we — can build other applications.

5.2. MPFR

Keywords: *Ieee 754*, *arbitrary precision*, *correct rounding*, *floating-point number*.

Participants: Guillaume Hanrot, Philippe Théveny, Paul Zimmermann [contact].

MPFR is one of the main pieces of software developed by the CACAO team. Since end 2006, with the departure of Vincent Lefèvre to ENS Lyon, it has become a joint project between CACAO and the ARENAIRE project-team (INRIA Grenoble - Rhône-Alpes). MPFR is a library for computing with arbitrary precision floating-point numbers, together with well-defined semantics, distributed under the LGPL license. In particular, all arithmetic operations are performed according to a rounding mode provided by the user, and all results are guaranteed correct to the last bit, according to the given rounding mode.

Several software systems use MPFR, for example: the GCC and GFORTRAN compilers; the SAGE computer algebra system; the KDE calculator Abakus by Michael Pyne; CGAL (Computational Geometry Algorithms Library) developed by the Geometrica project-team (INRIA Sophia Antipolis - Méditerranée); Gappa, by Guillaume Melquiond; Genius Math Tool and the GEL language, by Jiri Lebl; Giac/Xcas, a free computer algebra system, by Bernard Parisse; the iRRAM exact arithmetic implementation from Norbert Müller (University of Trier, Germany); the Magma computational algebra system; and the Wcalc calculator by Kyle Wheeler.

The main developments in 2007 were: (i) the start of the MPtools project (see below); (ii) the release of MPFR 2.3.0, which integrates new functions, among which the Bessel functions, on August 29; and (iii) the organization of the CEA-EDF-INRIA school *Certified Numerical Computation* on October 25-26 in Nancy[4], where Guillaume Hanrot and Paul Zimmermann gave the lectures on reliable floating-point computation and on MPFR. Also, the paper [6] summarizing the objectives, architecture, and features of MPFR has finally appeared.

In 2007, an ODL (*Opération de Développement Logiciel*) called MPtools was supported by INRIA for two years. A new engineer, Philippe Théveny, was hired in September. The objectives of the MPtools project are to add new mathematical functions to MPFR and MPC. As of October, the following new functions were already implemented: the arithmetic functions combining MPFR and the double type (`mpfr_add_d`, `mpfr_sub_d`, `mpfr_d_sub`, `mpfr_mul_d`, `mpfr_div_d`, `mpfr_d_div`), the `mpfr_modf` function (simultaneous integer and fractional part), the `mpfr_fmod` and `mpfr_remainder` functions (remainder of the division of two floating-point numbers, with different rounding modes), the `mpfr_fms` function (fused multiply and subtract), the `mpfr_sinh_cosh` function (simultaneous hyperbolic sine and cosine), the `mpfr_lgamma` function (logarithm of the gamma function), the J and Y Bessel functions.

[4] http://www.inria.fr/actualites/colloques/cea-edf-inria/2007/cnc/index.en.html

5.3. MPC

Keywords: *arbitrary precision*, *complex floating-point number*, *correct rounding*.

Participants: Philippe Théveny, Paul Zimmermann [contact].

MPC is a floating-point library for complex numbers, which is developed on top of the MPFR library, and distributed under the LGPL license. It is co-written with Andreas Enge (TANC team, INRIA Futurs Saclay). A complex floating-point number is represented by $x + iy$, where x and y are real floating-point numbers, represented using the MPFR library. The MPC library currently implements all basic arithmetic operations, the exponential and sine functions, all with correct rounding on both the real part x and the imaginary part y of any result. A new version, MPC 0.4.6, was released in 2007. MPC is used in particular in the TRIP celestial mechanics system developed at IMCCE (*Institut de Mécanique Céleste et de Calcul des Éphémérides*).

5.4. Gmp-Ecm

Participants: Pierrick Gaudry, Alexander Kruppa, Paul Zimmermann [contact].

GMP-ECM is a program to factor integers using the Elliptic Curve Method. Its efficiency comes both from the use of the GMP library, and from the implementation of state-of-the-art algorithms. GMP-ECM contains a library (LIBECM) in addition of the binary program (ECM). The binary program is distributed under GPL, while the library is distributed under LGPL, to allow its integration into other non-GPL software. For example, the Magma computational number theory software and the SAGE computer algebra system both use LIBECM.

In October 2005, this project moved to http://gforge.inria.fr. Since then and up to November 2007, there have been more than 5000 downloads. According to the "table of champions" maintained by Richard Brent[5], the ten largest ECM factors were found using GMP-ECM, including the current ECM record (67 digits).

GMP-ECM is used by many mathematicians and computer scientists to factor integers; for example it can be used to prove the primality of an integer, since several primality tests require to factor a given proportion of a number [23].

In June, a collaboration has started between Alexander Kruppa and Peter Montgomery; they are designing a new algorithm for the so-called Phase 2 of the $p + 1$ and $p - 1$ algorithms which can be seen as particular cases of ECM. Their new algorithm is currently being implemented and tested within GMP-ECM, and a new $p + 1$ record prime factor of 60 digits was set by this implementation in October. An article has been submitted [22].

In September, version 6.1.3 of GMP-ECM was released.

5.5. Local fields

Participant: Emmanuel Thomé [contact].

Mploc is a `C` library for computing in p-adic fields and their unramified extensions. The focus is mainly on $\mathbb{Z}_p$ for prime p, and unramified extensions of $\mathbb{Z}_2$. The ability to compute in these structures is important to several applications, such as point counting or building curves with a prescribed number of points.

The Mploc library is already distributed[6] and used, although several performance improvements are sought. The library presently gathers 8,000 lines of `C` source code.

5.6. Finite fields

Participants: Pierrick Gaudry, Emmanuel Thomé [contact].

[5] http://wwwmaths.anu.edu.au/~brent/ftp/champs.txt
[6] http://www.loria.fr/~thome/software/mploc

mp$\mathbb{F}_q$ is (yet another) library for computing in finite fields. The purpose of mp$\mathbb{F}_q$ is not to provide a software layer for accessing finite fields determined at runtime within a computer algebra system like Magma, but rather to give a very efficient, optimized code for computing in finite fields precisely known at *compile time*. mp$\mathbb{F}_q$ is not restricted to a finite field in particular, and can adapt to finite fields of any characteristic and any extension degree. However, one of the targets being use in cryptology, mp$\mathbb{F}_q$ somehow focuses on prime fields and on fields of characteristic two.

mp$\mathbb{F}_q$'s ability to generate specialized code for desired finite fields differentiates this library from its competitors. The performance achieved is far superior. For example, mp$\mathbb{F}_q$ can be readily used to assess the throughput of an efficient software implementation of a given cryptosystem. Such an evaluation is the purpose of the "EBats" benchmarking tool[7]. In 2007, several contributions based on mp$\mathbb{F}_q$ have been submitted to the "EBats" contest. In particular, the authors improved over the fastest examples of key-sharing software in genus 1 and 2, both over binary fields and prime fields.

The library's purpose being the *generation* of code rather than its execution, the working core of mp$\mathbb{F}_q$ consists of roughly 5,000 lines of Perl code, which generate most of the currently 13,000 lines of C code. mp$\mathbb{F}_q$ is currently under active development, and a first release is expected in early 2008. An article describing the mp$\mathbb{F}_q$ library and its use for implementing curve-based cryptosystems has been published [14].

5.7. Polynomial arithmetic in characteristic 2

Participants: Pierrick Gaudry, Emmanuel Thomé, Paul Zimmermann [contact].

Gf2x is a set of programs for polynomial multiplication over the binary field, developed together with Richard Brent (Australian National University, Canberra, Australia). There are implementations of various algorithms corresponding to different degrees of the input polynomials. In the case of polynomials that fit into one or two machine-words, the schoolbook algorithm has been improved and implemented using SSE instructions for maximum speed. For small degrees, we switch to Karatsuba's algorithm and then to Toom-Cook's algorithm. These have been implemented using the most recent improvements. Finally, for very large degrees one has to switch to Fourier-transform based algorithms, namely Schönhage's or Cantor's algorithm. In order to choose between these two asymptotically fast algorithms, we have implemented and compared them. A first release of GF2X, version 0.1, is available from http://wwwmaths.anu.edu.au/~brent/gf2x.html. In the long term, GF2X should be integrated within a more general library like NTL. An article describing our improvements to the algorithms and their implementation has been submitted, see [20].

5.8. MPQS

Participant: Paul Zimmermann.

MPQS is a program that factors integers using the Multiple Polynomial Quadratic Sieve, developed by Scott Contini and Paul Zimmermann. It is distributed under GPL from http://www.loria.fr/~zimmerma/free.

6. New Results

6.1. Floating-Point Arithmetic

Participants: Guillaume Hanrot, Philippe Théveny, Paul Zimmermann.

Two papers written in end-2006, on worst cases of periodic functions for large arguments, and on floating-point L^2 approximations to functions, have been published in 2007, see [10], [15].

The paper analyzing the error bounds on the complex floating-point multiplication finally appeared, see [4].

[7] http://www.ecrypt.eu.org/ebats/

6.2. Exact arithmetic

Participants: Pierrick Gaudry, Guillaume Hanrot, Alexander Kruppa, Emmanuel Thomé, Paul Zimmermann.

We have worked on Schönhage-Strassen's algorithm for multiplying very large integers. Starting with the GMP implementation, we have designed several improvements, some of them are more implementation tricks (like preserving locality in the computation to stay in the cache as much as possible), and some of them are algorithmic improvements (like combining a Mersenne- and a Fermat-like transform). These ideas have been published in [13], and the corresponding code is released under the LGPL license as a patch against the GMP library[8].

In collaboration with Cheng and Zima, see [11], we have improved upon the best known algorithms for computing hypergeometric constants. The theoretical asymptotical complexity is unchanged, but the practical behaviour is better. We demonstrated the efficiency by computing billions of digits of π and 2 billions of digits of $\zeta(3) := \sum_{n\geq 1} n^{-3}$, which is a new record[9].

Richard Brent and P. Zimmermann are collaborating on a book called "Modern Computer Arithmetic". A preliminary version [1] has been published on the web. An INRIA associate team[10] with Brent's group in Canberra will start in 2008, of which one of the goals is to work on that book.

Another common project with Richard Brent is the search for primitive trinomials over $\mathbb{F}_2$. A new factoring algorithm has been designed in this context, see [9], thus most of the operations are now squares which are very cheap in characteristic 2. One of our goals is to improve algorithms for finding primitive trinomials of degree a Mersenne prime. An implementation of the latter algorithm was first used to check our previous search for primitive trinomials of degree 6972593, one of the largest Mersenne primes known: we observed a speedup of a factor 70 over the previous algorithm. Then we searched for new primitive trinomials of degree 24036583, and we found exactly two (and their reciprocal):

$$x^{24036583} + x^{8412642} + 1, \quad x^{24036583} + x^{8785528} + 1.$$

The search for the next Mersenne exponent, 25964951, was performed using the idle cycles of the Grid 5000 platform ("besteffort" mode); four primitive trinomials were found:

$$x^{25964951} + x^{880890} + 1, x^{25964951} + x^{4627670} + 1, x^{25964951} + x^{4830131} + 1, x^{25964951} + x^{6383880} + 1.$$

All those primitive trinomials have been checked by Allan Steel using Magma. A journal paper [21] describing in detail the new algorithm has been accepted to a special issue of *Contemporary Mathematics*.

6.3. Crypto-related results

Participants: Pierrick Gaudry, Guillaume Hanrot, Emmanuel Thomé, Marion Videau.

6.3.1. Constructive results

In the context of genus 2 cryptography, we have designed fast explicit formulæ for the group law in the Jacobian; in fact the formulæ work in the so-called Kummer surface, that is a point and its opposite are merged into a single element. The Kummer surface is not a group, but there is still enough structure to add an element with itself, and then to build cryptosystems. Our formulæ are much faster than previously known formulæ for genus 2 arithmetic. For the case of odd characteristic, the resulting algorithm has been published in [7]. The formulæ have been extended to characteristic 2. Although they do work in all examples we have tested, a rigorous proof of their validity is yet to be found. All these algorithms have been implemented on top of the $\texttt{mp}\mathbb{F}_q$ library, thus confirming that genus 2 cryptosystems can be faster than elliptic ones. This implementation has been the subject of a publication, see [14].

[8] http://www.loria.fr/~kruppaal/mul_fft-4.2.1.1.tgz
[9] http://numbers.computation.free.fr/Constants/constants.html
[10] http://www.loria.fr/~zimmerma/anc.html

Another "constructive" work has been done in collaboration with Laurent Théry. The goal was to give a rigorous proof of the primality of an integer. There exist software tools that produce elliptic certificates of primality, for instance, `fastECPP` written by François Morain. The algorithm for checking the certificates is much simpler than for producing it, and it has been possible to implement it within `Coq`. This implementation is described in [19].

6.3.2. Destructive results

The paper written on the algorithm developed in 2005 (using a double large prime variation for the discrete logarithm problem, DLP for short, in Jacobian of curves) with Gaudry, Thomé, Diem and Thériault has been published [8].

The improvement by Diem in the case of small degree curves has been more precisely studied by Diem and Thomé who improved the heuristic proof towards a more rigorous one, where the only remaining heuristic argument is reduced to a random graph comparison result. That paper will be published in *Journal of Cryptology*, and is already electronically published [5].

Another contribution in the context of discrete logarithms has been obtained by Enge and Gaudry. For a general curve of large enough genus g over a finite field q, the complexity of a discrete log computation is in $L_{q^g}(1/2)$, where $L()$ is the classical subexponential function (this has been recently proven in a rigorous way by Hess [25]). Enge and Gaudry [12] have shown that for plane curves having a particular shape of degrees in x and y, this complexity can been reduced heuristically to $L_{q^g}(1/3+\varepsilon)$, recovering the kind of complexity we have for integer factorization or discrete logarithms in finite fields. We are now working on removing the ε in the complexity.

Concerning lattices, Hanrot and Stehlé (ARENAIRE project-team, INRIA Grenoble - Rhône-Alpes) completed an analysis of Kannan's enumeration algorithm, the best deterministic algorithm for finding a shortest non-zero vector in a lattice, or a closest vector to a given point. They proved that, in contradiction to what was believed since the beginning of the 90's, the complexity of the former problem is at most $d^{d/(2e)+o(d)}$ arithmetic operations on integers of polynomial size (instead of $d^{d/2+o(d)}$); for the latter problem, the complexity drops from $d^{d+o(d)}$ to $d^{d/2+o(d)}$. These analysis more generally yield results on the complexity of HKZ-reduction, which is also $d^{d/(2e)+o(d)}$. This work was presented at the Crypto'07 conference, see [16].

Using an adaptation of the Number Field Sieve algorithm, Joux, Naccache and Thomé obtained a variety of new signature forgery algorithms for the RSA digital signature algorithm, when one uses *affine padding* (where one uses e.g., $(c+x)^d$ as the signature of a message x). The basic assumption is that the attacker has access to an oracle providing modular e-th roots of the form $\sqrt[e]{c+x}$. Within subexponential complexity, it is shown that additional such roots can be obtained. The attack has the same complexity as the *special* Number Field Sieve algorithm, which is much lower than the *general* Number Field Sieve. Another result of this work is a new subexponential algorithm solving the *one-more-rsa* problem. This work was presented at the Asiacrypt 2007 conference, see [17].

6.3.3. Legal aspects

2007 was last year for the project Asphalès which had been selected for funding in 2004 by ACI Sécurité et Informatique. The project goal is the study of the interaction between information security and legal safeguards. Marion Videau coordinates the projet, jointly with Isabelle de Lamberterie and Stéphanie Lacour. She has worked on the probative value of electronic data media and their conservation. The article "Légistique de l'écrit électronique", results of a joint work with Stéphanie Lacour (CNRS-CECOJI / OCDE-Working Party on Nanotechnology) has been published [18] among other contributions from various workshops held during Asphalès project lifetime by l'Harmattan in a book entitled "La Sécurité aujourd'hui dans la société de l'information".

Marion Videau and Stéphanie Lacour continue their joint work on various aspects of information security (personal medical data files, nanotechnology development).

7. Contracts and Grants with Industry

7.1. MPQS

Participant: Paul Zimmermann.

A non-exclusive license contract (CACAO-LICENCE MPQS-2680) has been signed on July 25th with Waterloo Maple Inc. (WMI), to enable the use of a fixed version of MPQS (see Section 5.8) within the Maple computer algebra software.

8. Other Grants and Activities

8.1. National Initiatives

8.1.1. ANR CADO (Crible algébrique, Distribution, Optimisation)

Participants: Pierrick Gaudry, Guillaume Hanrot, Alexander Kruppa, Emmanuel Thomé, Paul Zimmermann.

The team has obtained a financial support from the ANR ("programme blanc") for a project, common with the TANC project-team and the number theory team of the mathematics lab in Nancy (IECN). Its objective is to study the number field sieve algorithm.

We are working on several aspects of this factoring algorithm, that are linked to our main objectives. Among other things, we will investigate the so-called "polynomial selection" phase, which could possibly be improved using some lattice reduction tools, we will work on the parallelization (in a Grid context) of the linear algebra step, we also want to study the relation search phase, where the speed of the underlying arithmetic is crucial.

For all of that, it is important to us to have our own implementation. Therefore, we have started the writing of this implementation, that will be released under a free software license. The main goal is not to break records, but to have a convenient and configurable tool to test different strategies.

8.1.2. ANR RAPIDE (Conception et analyse de chiffrements à flots efficaces pour les environnements contraints)

Participants: Guillaume Hanrot, Marion Videau, Paul Zimmermann.

The project RAPIDE has begun January 1st, 2007. RAPIDE's goal is the study of the design and the analysis of efficient stream ciphers suitable for constrained environments. It has been granted and partially funded by the ANR during the SETIN 2006 call for proposals. Marion Videau is the head of this project. Guillaume Hanrot and Paul Zimmermann take part in the research activity.

The research activity is centered around the question of non-linear feedback functions. The idea is either to find a suitable way to use symmetric Boolean functions as feedback functions since they are well known for their good implementation properties or to find a way to synthesize new families of Boolean functions having both good cryptographic parameters and good implementation characteristics.

To improve the knowledge about symmetric Boolean functions and their potential use as nonlinear feedbacks, Marion Videau is currently working in collaboration with the university of Bergen, Selmer Center, Norway. Symmetric Boolean functions have indeed good representation properties that are currently studied in collaboration with Matthew G. Parker in order to apply them to quantum codes. Contacts have also been taken with Johannes Mykkeltveit for the study of sequences generated with symmetric feedbacks. On the synthesis side, Marion Videau is currently working with Cédric Lauradoux (post-doctoral fellow, Princeton University) on the properties of a special class of partially symmetric functions (a paper is currently submitted).

8.2. International Initiatives

8.2.1. Collaboration with ANU

Participants: Richard Brent, Paul Zimmermann.

Richard Brent visited the CACAO team in May. This visit led to new results concerning the arithmetic of binary polynomials. To reinforce the active collaboration with Richard Brent and his team, an "associate team" ANC (Algorithms, Numbers, Computers) has been proposed, and supported by INRIA[11].

8.2.2. Other visits

Florian Hess from TU Berlin visited us in January, working mainly with P. Gaudry on efficient group laws in Jacobians of curves. David Kohel from University of Sydney has spent 2 months in May/June with the CACAO team as an invited professor of Université Henri Poincaré. He was then hired as a professor in Marseille, and this visit has been a good opportunity to establish good relations with the new group he is starting there. Dan Bernstein and Tanja Lange from TU Eindhoven have visited us at the end of November to work on various topics, including integer factorisation and curve based cryptography.

Marion Videau has spent one month (July 2007) in Bergen, with Selmer Center, in order to develop common projects with the group of coding theory and cryptography which is worlwide renown in the field.

Guillaume Hanrot spent three weeks together with Nicolas Brisebarre (ARENAIRE project-team) at the Tsukuba University in order to prepare a collaboration on pairing computation, in software and hardware. A joint proposal has been submitted to the PHC Sakura program. The results are pending.

9. Dissemination

9.1. Scientific Animation

9.1.1. CACAO seminar

We have a seminar, where we have invited in 2007 the following speakers: Jean-Luc Beuchat, Richard Brent, Sylvain Chevillard, Jeremie Detrey, Christophe Doche, David Kohel, Christoph Lauter, David Lubicz, Guillaume Melquiond, Clément Pernet, Thomas Sirvent, Ben Smith, Ley Wilson.

9.1.2. Conference organization

Emmanuel Thomé has co-organized the *Journées Nationales de calcul Formel*, that took place in Luminy in January. He will also co-organize the next meeting in 2008.

Pierrick Gaudry has co-organized the *École Jeunes Chercheurs en Informatique Mathématique*, that took place in Nancy in March.

Guillaume Hanrot and Paul Zimmermann have organized the 1st school on *Certified Numerical Computation* on October 25-26 in Nancy[12], which attracted 14 participants from research institutes, universities and industry.

9.2. Leadership within Scientific Community

Guillaume Hanrot was in the Program Committee of the ISSAC 2007 conference; Paul Zimmermann was in the Program Committee of the ARITH 18 conference; both are members of the steering committee of the RNC conference. Pierrick Gaudry was in the Program Committee of the WAIFI 2007 conference.

9.3. Committees memberships

G. Hanrot is vice-head of the Project Committee of INRIA Lorraine. He is also an appointed member of the INRIA Commission d'Évaluation, of the Mathematics "Commissions de Spécialistes" from Universités Montpellier 2, Henri Poincaré Nancy 1-Nancy 2-INPL, Jean-Monnet Saint-Étienne. He was a member of the hiring committee for CR2 at INRIA Rocquencourt in 2007.

[11] http://www.loria.fr/~zimmerma/anc.html
[12] http://www.inria.fr/actualites/colloques/cea-edf-inria/2007/cnc/index.en.html

P. Gaudry is an appointed member of the Computer Science “Commissions de Spécialistes” from Universités Henri Poincaré Nancy 1 and Paris 8. He was one of the reviewers of the PhD these of J. Pujolas (Universitat Politècnica de Catalunya, Barcelona).

P. Zimmermann is an elected member from the INRIA Evaluation Committee, and of the Computer Science “Commission de Spécialistes” from University Henri Poincaré Nancy 1. He was member of the PhD thesis jury of Marc Glisse (Univ. Nancy 2), of Romain Péchoux (INPL), and of the habilitation jury of Isabelle Debled-Rennesson (Univ. Henri Poincaré Nancy 1). He was a member of the hiring committee for CR2 at INRIA Futurs Saclay in 2007.

9.4. Invited Conferences

G. Hanrot gave a one-hour invited talk for the LLL+25 conference, Caen, and wrote a survey on the topic of his talk, which shall be published in a proceedings volume. P. Gaudry gave a one-hour invited talk for the “Computational Challenges Arising in Algorithmic Number Theory and Cryptography Workshop”, Toronto and a one-hour invited talk for the ECC 2007 conference, Dublin. Paul Zimmermann gave invited talks at the “Conference on Algorithmic Number Theory” in Turku (Finland), at the “Explicit Methods and Number Theory” conference in Bordeaux (France), and at the SAGE Days 6 in Bristol (United Kingdom). M. Videau gave an invited talk at the C&ESAR 2007 (Computer & Electronics Security Applications Rendez-vous).

9.5. Teaching

As an assistant professor, M. Videau teaches mainly at the master level. The courses directly related to her research activities are : *Introduction to cryptography* (master degree, engineering school) and *Introduction to the security of communicating systems* (master degree). She has supervised the master thesis of Pierre Dégardin (University of Limoges), entitled “Is it possible to replace the S-box of the AES by a binomial or trinomial permutation function?”.

P. Gaudry gave three 3 hours lectures at MPRI (Master Parisien de Recherche en Informatique) about algorithmic number theory, in the Cryptology course.

E. Thomé gave 6 hours of computer lab at Université Henri Poincaré (M1 students) on the topic of the security of communicating systems.

P. Gaudry and G. Hanrot are members of the jury of “agrégation externe de mathématiques”, a competitive exam to hire high school teachers.

E. Thomé is a member of the jury of the competitive exam for the École polytechnique.

10. Bibliography

Major publications by the team in recent years

[1] R. P. BRENT, P. ZIMMERMANN. *Modern Computer Arithmetic*, In preparation. Current version available at http://www.loria.fr/~zimmerma/mca/pub226.html, Version 0.1.1, 2006.

[2] D. DEFOUR, G. HANROT, V. LEFÈVRE, J.-M. MULLER, N. REVOL, P. ZIMMERMANN. *Proposal for a Standardization of Mathematical Function Implementation in Floating-Point Arithmetic*, in "Numerical Algorithms", vol. 37, n^{o} 1-2, 2004, p. 367–375, http://hal.inria.fr/inria-00071249/en/.

Year Publications

Articles in refereed journals and book chapters

[3] A. BOSTAN, P. GAUDRY, E. SCHOST. *Linear recurrences with polynomial coefficients and application to integer factorization and Cartier-Manin operator*, in "SIAM Journal on Computing", vol. 36, 2007, p. 1777-1806, http://hal.inria.fr/inria-00103401/en/.

[4] R. BRENT, C. PERCIVAL, P. ZIMMERMANN. *Error Bounds on Complex Floating-Point Multiplication*, in "Mathematics of Computation", vol. 76, 2007, p. 1469-1481, http://hal.inria.fr/inria-00120352/en/.

[5] C. DIEM, E. THOMÉ. *Index calculus in class groups of non-hyperelliptic curves of genus three*, in "Journal of Cryptology", The original publication is available at www.springerlink.com, 2007, http://hal.inria.fr/inria-00107290/en/.

[6] L. FOUSSE, G. HANROT, V. LEFÈVRE, P. PÉLISSIER, P. ZIMMERMANN. *MPFR: A Multiple-Precision Binary Floating-Point Library wit h Correct Rounding*, in "ACM Transactions on Mathematical Software", Article 13, 15 pages, vol. 33, n^{o} 2, June 2007, 13, http://doi.acm.org/10.1145/1236463.1236468.

[7] P. GAUDRY. *Fast genus 2 arithmetic based on Theta functions*, in "Journal of Mathematical Cryptology", vol. 1, 2007, p. 243-265, http://hal.inria.fr/inria-00000625/en/.

[8] P. GAUDRY, E. THOMÉ, N. THÉRIAULT, C. DIEM. *A double large prime variation for small genus hyperelliptic index calculus*, in "Mathematics of Computation", vol. 76, 2007, p. 475-492, http://hal.inria.fr/inria-00000897/en/.

Publications in Conferences and Workshops

[9] R. BRENT, P. ZIMMERMANN. *A Multi-level Blocking Distinct Degree Factorization Algorithm*, in "8th International Conference on Finite Fields and Applications (Fq8), Melbourne Australie", 2007, http://hal.inria.fr/inria-00187614/en/.

[10] N. BRISEBARRE, G. HANROT. *Floating-Point L^2-Approximations*, in "18th IEEE Symposium in Computer Arithmetic, Montpellier France", P. KORNERUP, J.-M. MULLER (editors), IEEE, 2007, p. 177-186, http://hal.inria.fr/inria-00119254/en/.

[11] H. CHENG, G. HANROT, E. THOMÉ, E. ZIMA, P. ZIMMERMANN. *Time- and Space-Efficient Evaluation of Some Hypergeometric Constants*, in "International Symposium on Symbolic and Algebraic Computation - ISSAC'07 Proceedings of the 2007 international symposium on Symbolic and algebraic computation, Waterloo Canada", ISBN: 978-1-59593-743-8, ACM, Association for Computing Machinery, 2007, p. 85-91, http://hal.inria.fr/inria-00177850/en/.

[12] A. ENGE, P. GAUDRY. *An $L(1/3+\varepsilon)$ Algorithm for the Discrete Logarithm Problem for Low Degree Curves*, in "Eurocrypt 2007 Advances in Cryptology - EUROCRYPT 2007 Lecture Notes in Computer Science, Barcelona Espagne", M. NAOR (editor), Lecture Notes in Computer Science, vol. 4515, Springer, 2007, p. 379-393, http://hal.inria.fr/inria-00135324/en/.

[13] P. GAUDRY, A. KRUPPA, P. ZIMMERMANN. *A GMP-based implementation of Schönhage-Strassen's large integer multiplication algorithm*, in "ISSAC 2007 Proceedings of the 2007 international symposium on

Symbolic and algebraic computation, Waterloo, Ontario Canada", C. W. BROWN (editor), ACM Press, 2007, p. 167-174, http://hal.inria.fr/inria-00126462/en/.

[14] P. GAUDRY, E. THOMÉ. *The mpFq library and implementing curve-based key exchanges*, in "SPEED: Software Performance Enhancement for Encryption and Decryption, Amsterdam Pays-Bas", ECRYPT Network of Excellence in Cryptology, 2007, p. 49-64, http://hal.inria.fr/inria-00168429/en/.

[15] G. HANROT, V. LEFÈVRE, D. STEHLÉ, P. ZIMMERMANN. *Worst Cases of a Periodic Function for Large Arguments*, in "18th IEEE Symposium in Computer Arithmetic, Montpellier France", P. KORNERUP, J.-M. MULLER (editors), IEEE, 2007, p. 133-140, http://hal.inria.fr/inria-00126474/en/.

[16] G. HANROT, D. STEHLÉ. *Improved Analysis of Kannan's Shortest Lattice Vector Algorithm*, in "Advances in Cryptology - Crypto'07 LNCS, Santa Barbara États-Unis d'Amérique", A. MENEZES (editor), LNCS, vol. 4622, Springer-Verlag, 2007, p. 170-186, http://hal.inria.fr/inria-00145049/en/.

[17] A. JOUX, D. NACCACHE, E. THOMÉ. *When e-th Roots Become Easier Than Factoring*, in "13th International Conference on the Theory and Application of Cryptology and Information Security - ASIACRYPT 2007 Advances in Cryptology – ASIACRYPT 2007 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, December 2-6, 2007. Proceedings Lecture Notes in Computer Science, Kuching Malaisie", K. KUROSAWA (editor), Lecture Notes in Computer Science, The original publications is available at www.springerlink.com ; ISBN 978-3-540-76899-9 ; ISSN 0302-9743 (Print) 1611-3349 (Online), vol. 4833, Springer Berlin / Heidelberg, International Association for Cryptologic Research, 2007, p. 13-28, http://hal.inria.fr/inria-00187782/en/.

[18] S. LACOUR, M. VIDEAU. *Légistique de l'écrit électronique*, in "Séminaire « Preuve, archivage et conservation électroniques », Paris France", L'Harmattan, 2007, p. 183–208, http://hal.archives-ouvertes.fr/hal-00187831/en/.

[19] L. THÉRY, G. HANROT. *Primality Proving with Elliptic Curves*, in "TPHOL 2007 Theorem Proving in Higher Order Logics LNCS, Kaiserslautern Allemagne", K. SCHNEIDER, J. BRANDT (editors), LNCS, vol. 4732, Springer-Verlag, 2007, p. 319-333, http://hal.inria.fr/inria-00138382/en/.

Internal Reports

[20] R. BRENT, P. GAUDRY, E. THOMÉ, P. ZIMMERMANN. *Faster Multiplication in GF(2)[x]*, Research Report, n^{o} RR-6359, 2007, http://hal.inria.fr/inria-00188261/en/.

[21] R. BRENT, P. ZIMMERMANN. *A Multi-level Blocking Distinct Degree Factorization Algorithm*, Research Report, n^{o} RR-6331, INRIA, 2007, http://hal.inria.fr/inria-00181029/en/.

Miscellaneous

[22] P.-L. MONTGOMERY, A. KRUPPA. *Improved Stage 2 to P±1 Factoring Algorithms*, 2007, http://hal.inria.fr/inria-00188192/en/.

References in notes

[23] B. GRÉGOIRE, L. THÉRY, B. WERNER. *A computational approach to Pocklington certificates in type theory*, in "Proceedings of FLOPS'06", Lecture Notes in Comput. Sci., vol. 3945, Springer–Verlag, 2006.

[24] C. HERMITE. *Extraits de lettres de M. Hermite à M. Jacobi sur différents objets de la théorie des nombres, deuxième lettre*, in "Journal für die reine und angewandte Mathematik", vol. 40, 1850, p. 279–290.

[25] F. HESS. *Computing relations in divisor class groups of algebraic curves over finite fields*, Preprint, 2004.

[26] IEEE. *P1363: Standard specifications for public key cryptography*, Available at http://www.manta.ieee.org/groups/1363/.

[27] N. KOBLITZ. *Elliptic curve cryptosystems*, in "Math. Comp.", n^{o} 48, 1987, p. 203–209.

[28] A. K. LENSTRA, H. W. LENSTRA, L. LOVÁSZ. *Factoring Polynomials with Rational Coefficients*, in "Mathematische Annalen", vol. 261, 1982, p. 515–534.

[29] V. S. MILLER. *Use of Elliptic Curves in Cryptography*, in "Advances in cryptology—CRYPTO 85, New York, USA", Lecture notes in computer science, vol. 218, Springer-Verlag, 1986, p. 417–426.

[30] C. P. SCHNORR. *A Hierarchy of Polynomial Lattice Basis Reduction Algorithms*, in "Theoret. Comput. Sci.", vol. 53, 1987, p. 201–224.