INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team CACAO

Curves, Algebra, Computer Arithmetic, and so On

Nancy - Grand Est

Theme : Algorithms, Certification, and Cryptography

Table of contents

1. Team

Research Scientist

Jérémie Detrey [Research Scientist, INRIA]
Pierrick Gaudry [Research Scientist, CNRS; Team Leader since July 1st, HdR]
Guillaume Hanrot [Team Leader, Research Director, INRIA, until June 30th, HdR]
Emmanuel Thomé [Research Scientist, INRIA]
Paul Zimmermann [Research Director, INRIA, HdR]

Faculty Member

Marion Videau [assistant professor, Université Henri Poincaré; on secondment to ANSSI until January 2011]

Technical Staff

Lionel Muller [ADT grant, INRIA, from November 1st]
Philippe Théveny [ODL grant, INRIA, until August 31st]

PhD Student

Gaëtan Bisson [MESR grant, INPL and Technische Universiteit Eindhoven; defense planned in 2011]
Romain Cosset [INRIA/DGA grant; defense planned in 2011]
Nicolas Estibals [Master project student, February–June; Contrat doctoral, Université Henri Poincaré, since September 1st; defense planned in 2012]
Alexander Kruppa [CNRS grant; defense planned in January 2010]
Damien Robert [MESR grant, Université Henri Poincaré; defense planned in 2010]

Post-Doctoral Fellow

Sylvain Chevillard [Since September 1st]
Antonio Vera [Since February 1st]

Administrative Assistant

Emmanuelle Deschamps

Other

Răzvan Bărbulescu [Master project student, June–September]
Cyril Bouvier [Internship, June–July]
Iram Chelli [Master project student, April–September]

2. Overall Objectives

2.1. Introduction

The context of the research interests of the CACAO project-team goes with numbers and equations. We deal with mathematical objects of varying complexity, and strive for providing fast algorithms for manipulating them. In particular, *algebraic curves* over finite fields form a very important class of objects for our study, given their relevance to number theory and public-key cryptology.

The objectives of the CACAO 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-point 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 logarithm algorithms.

2.2. Highlights of the year

The highlights for year 2009 in the CACAO project-team are:

- J. Detrey and N. Estibals received the Best Paper Award at the CHES 2009 conference for their paper on hardware accelerators for the Tate pairing [8], in collaboration with J.-L. Beuchat and E. Okamoto (LCIS, University of Tsukuba, Japan); and F. Rodríguez-Henríquez (CINVESTAV, IPN, Mexico).
- The departure of our team leader Guillaume Hanrot, who joined the Arenaire project-team in Lyon in October.

3. Scientific Foundations

3.1. 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 [25] and Miller [27] 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.

3.2. 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 [26] 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 (HKZ) reduction [23], which require exponential or super-exponential time but solve the shortest vector problem in an exact way. Schnorr [28] introduced a complete hierarchy of reductions ranging from LLL to HKZ both in quality and in complexity, the so-called k-BKZ reductions.

3.3. Arithmetic

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 multiple-precision 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 revised standard 754-2008 is no more restricted to the 4 basic field operations and the square root, but recommends correct rounding for some mathematical functions, and also recommends how to extend the default available formats. This leads to efficiency questions, in particular to guarantee that the result of an operation has been correctly rounded in arbitrary precision.

Within the context of integer arithmetic, we are also interested in putting the problem on its head, and notably by the study of the converse operation to integer multiplication, that is, integer factoring. Being the most competitive algorithm for this task, the Number Field Sieve algorithm comes naturally as a context where several parts of our work find a natural continuation, in all of the three axes above.

4. Application Domains

4.1. 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 [24]) 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.

4.2. 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, Pari/GP, and Sage software tools.

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 an 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 strong community of active developers around Sage. This system is a good alternative to Maple, Mathematica, and Magma to better disseminate our research in the future.

4.3. Arithmetics

Another indirect transfer is the usage of MPFR in GFORTRAN (since 2004), and in GCC, up from version 4.3 (released in 2008). MPFR is currently used at compile-time, to convert expressions like $\sin(3.1416)$ into fixed-precision IEEE 754 formats, when the rounding mode can be statically determined. The MPFR library is also used by the CGAL library for computational geometry developed by the Geometrica project-team (INRIA Sophia Antipolis - Méditerranée).

The future release 4.5 of GCC will also require the MPC library; similarly to MPFR, MPC will be used to fold at compile-time constant expressions involving complex floating-point numbers.

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

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, and is 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.

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

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 2009 were: the release of version 2.4.0 (andouillette sauce moutarde) in January, with the new name GNU MPFR, the release of GNU MPFR 2.4.1 in February, the CNC'2 summer school in June, and the end of the contract of Philippe Théveny in September.

All those developments were done in the context of the ODL (*Opération de Développement Logiciel*) MPtools, supported by INRIA from September 2007 to August 2009.

5.3. MPC

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 (LFANT project-team, INRIA Bordeaux - Sud-Ouest). 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 provides correct rounding on both the real part x and the imaginary part y of any result. MPC is used in particular in the TRIP celestial mechanics system developed at IMCCE (*Institut de Mécanique Céleste et de Calcul des Éphémérides*), and by the Magma computational number theory system.

In 2009, in the context of the MPtools project, the focus was made on extending the list of available functions, to provide all functions of the C99 standard. A new version, MPC 0.6 (Bellis perennis) was released in April, MPC 0.7 (Campanula uniflora) was released in September, and MPC 0.8 (Dianthus deltoides) was released in November. Since May 2009, MPC is used optionally by GCC 4.4 to compute constant complex expressions at compile-time (constant folding), and since December 6, 2009, MPC is required for the development version of GCC (thus for the next release GCC 4.5).

5.4. Gmp-Ecm

Participants: Romain Cosset, 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 to 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 2009, GMP-ECM 6.2.2 and 6.2.3 have been released. In addition, the HECM implementation by Romain Cosset has been included in GMP-ECM.

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

[4] http://www.loria.fr/~thome/software/mploc

5.6. Finite fields

Participants: Pierrick Gaudry, Emmanuel Thomé [contact].

$\texttt{mp}\mathbb{F}_q$ is (yet another) library for computing in finite fields. The purpose of $\texttt{mp}\mathbb{F}_q$ 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*. $\texttt{mp}\mathbb{F}_q$ 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 the use in cryptology, $\texttt{mp}\mathbb{F}_q$ somehow focuses on prime fields and on fields of characteristic two.

$\texttt{mp}\mathbb{F}_q$'s ability to generate specialized code for desired finite fields differentiates this library from its competitors. The performance achieved is far superior. For example, $\texttt{mp}\mathbb{F}_q$ 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[5]. $\texttt{mp}\mathbb{F}_q$ entered this trend in 2007, establishing reference marks for fast elliptic curve cryptography: the authors improved over the fastest examples of key-sharing software in genus 1 and 2, both over binary fields and prime fields. These timings are now comparison references for other implementations [29].

The library's purpose being the *generation* of code rather than its execution, the working core of $\texttt{mp}\mathbb{F}_q$ consists of roughly 18,000 lines of Perl code, which generate most of the `C` code. Some part of $\texttt{mp}\mathbb{F}_q$ is distributed at http://mpfq.gforge.inria.fr/.

In 2009, some experimental code for polynomials over prime fields has been added to $\texttt{mp}\mathbb{F}_q$. Although not yet distributed it has been used for the record in genus 2 point counting (see below).

5.7. Polynomial arithmetic in characteristic 2

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

GF2X is a software library 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. The GF2X package is distributed and maintained. It is available from http://gforge.inria.fr/projects/gf2x/. The software library NTL, as of version 5.5 (April 2009) can be configured to use GF2X as an auxiliary package for best performance. NTL being a very widespread library across the community, it is thus expected that GF2X will thus be used in e.g., SAGE shortly. Documentation on the link between NTL and GF2X can be obtained from http://www.shoup.net/ntl/doc/tour-gf2x.html. Work on GF2X was part of the ANC associate team (see below).

5.8. CADO-NFS

Participants: Cyril Bouvier, Jérémie Detrey, Pierrick Gaudry, Alexander Kruppa, Lionel Muller, Emmanuel Thomé [contact], Antonio Vera, Paul Zimmermann.

CADO-NFS is a program to factor integers using the Number Field Sieve algorithm (NFS), developped in the context of the ANR-CADO project.

NFS is a complex algorithm which contains a large number of sub-algorithms. The implementation of all of them is now complete, but still leaves many places to be improved. Compared to existing implementations, the CADO-NFS implementation is already a reasonable player. Several factorizations have been completed using our implementations.

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

In 2009, the linear algebra code in CADO-NFS (which uses the block Wiedemann algorithm) has been reprogrammed mostly from scratch in C, and now works as a multi-thread, multi-node implementation, using both POSIX threads and the MPI interface. A number of algorithms have been implemented for the basic matrix times vector multiplications, which account for the largest share of the computation time.

During the sieving step of NFS a great number of smaller integers need to be factored. For this task an implementation of the P–1, P+1 and Elliptic Curve factoring methods has been written, optimized for high-throughput factorization of relatively small numbers (unlike GMP-ECM, which uses asymptotically fast algorithms to find factors as large as possible with these algorithms). The code is competitive in terms of performance/cost-ratio with recently proposed hardware implementations of ECM for NFS. The details of the implementation are published in the research report [15].

In 2009, the CADO-NFS program has been made available publicly from http://cado-nfs.gforge.inria.fr/. New versions of programs for the filtering step have been designed — with the help of Cyril Bouvier — for the factorization of RSA-768; those programs will be integrated within CADO-NFS by Lionel Muller.

6. New Results

6.1. Floating-Point Arithmetic

Participants: Guillaume Hanrot, Philippe Théveny, Paul Zimmermann.

Together with Siegfried Rump, Sylvie Boldo and Guillaume Melquiond, P. Zimmermann published a new efficient algorithm to compute the predecessor or successor of a floating-point number in rounding to nearest mode [7]. This algorithm is about two times faster than the `nextafter` function from the GNU C library.

With Vincent Lefèvre from the Arenaire project-team, and Kaveh Ghazi (GCC developer), Ph. Théveny and P. Zimmermann submitted an article entitled *Why and how to use arbitrary precision* to the journal *Computing in Science and Engineering*.

6.2. Exact arithmetic

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

Richard Brent and P. Zimmermann are collaborating on a book called “Modern Computer Arithmetic”. Three new versions (0.2.1 in March, 0.3 in June, and 0.4 in November) have been published in 2009, in the context of the INRIA ANC associate team[6] which started in 2008. Version 0.4 includes feedback from two anonymous reviewers for a commercial publisher.

Another common project with Richard Brent is the search for primitive trinomials over $\mathbb{F}_2$. While the paper corresponding to degrees 24036583, 25964951, 30402457, and 32582657 appeared [2], the search for primitive trinomials corresponding to huge Mersenne primes continued. For degree 43112609, we have found four primitive trinomials (and their reciprocal):

$$x^{43112609} + x^{3569337} + 1, x^{43112609} + x^{4463337} + 1, x^{43112609} + x^{17212521} + 1, x^{43112609} + x^{21078848} + 1,$$

and for degree $r = 42643801$, we have found exactly five:

$$x^r + x^{55981} + 1, x^r + x^{3706066} + 1, x^r + x^{3896488} + 1, x^r + x^{12899278} + 1, x^r + x^{20150445} + 1.$$

[6] http://www.loria.fr/~zimmerma/anc.html

All those primitive trinomials have been checked by Allan Steel using Magma. Those results will be published in an invited paper to the AMS Notices.

Together with Will Orrick (Indiana University) and Judy-anne Osborn (Australian National University), Richard Brent and P. Zimmermann started another project on maximal determinants of Hadamard matrices. Results so far include the fact that the conjectured maximal determinant for $n = 19$ is the true maximal determinant, and similarly for $n = 37$. This work was done with the support of the ANC associate team too.

Together with Philippe Dumas, Claude Gomez and Bruno Salvy, P. Zimmermann published an electronic version of the book "Calcul formel : mode d'emploi. Exemples en Maple" (in french), previously published by a commercial editor, and whose rights have been given back to the authors [12].

6.3. Curve-related results

Participants: Răzvan Bărbulescu, Gaëtan Bisson, Iram Chelli, Romain Cosset, Pierrick Gaudry, Guillaume Hanrot, Damien Robert, Emmanuel Thomé.

Over the winter, Gaëtan Bisson has been working jointly with Andrew V. Sutherland (Massachusetts Institute of Technology) on new algorithms for computing endomorphism rings of ordinary elliptic curves over finite fields [18]. Endomorphism rings are relevant security parameters for elliptic-curve-based cryptosystems and are also very involved with the CM method for curve generation. The new algorithms outperform Kohel's algorithm (the previous state-of-the-art method) both asymptotically and in practice; it also satisfyingly answers the problem of certifying such endomorphism rings.

During his master project internship, Iram Chelli has designed a fully deterministic ECM algorithm [14]. For example, 124 well-chosen Suyama curves with bounds $B_1 = 260$ and $B_2 = 11600$ enable one to find all prime factors up to 2^{32} in any composite integer.

Răzvan Bărbulescu has found two infinite sub-families of Suyama curves for which the probability to give a factorization is higher [16]. This result is based on the observation by Kruppa of some weird behaviour of a few Suyama curves.

Romain Cosset has worked on developing a genus-2 "hyperelliptic curve method" for integer factoring [3], as an extension to the well-known elliptic curve method. The implementation GMP-HECM of this algorithm is faster than GMP-ECM for factoring big numbers (at least 250 digits).

Damien Robert and David Lubicz have worked on explicit isogeny computation in genus 2. With Jean-Charles Faugère, they have defined a modular correspondance between abelian varieties [21]. Then they have designed an algorithm, similar to the so-called Vélu's formulae for elliptic curves, that uses this modular correspondence to construct explicit isogenies between abelian varieties. They have also found a new algorithm to compute the Weil pairing on an abelian variety. Two articles will be written in 2009–2010 describing these algorithms.

Pierrick Gaudry and Éric Schost finished a record-setting computation of a so-called doubly-secure genus 2 curve for cryptographic use. The computation is based on their previous experiment of Spring 2008, where a single curve was computed. The software has been improved – some critical parts now use the $\texttt{mp}\mathbb{F}_q$ library – and has been run on thousands of curves until one with good cryptographic properties was obtained. They used the Sharcnet grid facility[7], on which they obtained a "Dedicated Ressource" grant of one and a half million hours. This result has been announced in oral communications at conferences, and a journal paper is under writing.

Andreas Enge, Pierrick Gaudry and Emmanuel Thomé have finished their common article describing a class of curves for which they give a discrete logarithm algorithm with heuristic complexity $L_{q^g}(1/3)$, where g is the genus and q the cardinality of the finite field. The article has been accepted to Journal of Cryptology [19].

The article [6] by Gaudry and Lubicz about efficient arithmetic in Kummer surfaces has been accepted and published.

[7] http://www.sharcnet.ca

6.4. Number Field Sieve-related results

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

The team has been involved in the factorization of RSA-768, a 768-bit integer. With the usage of Grid'5000 computers in "besteffort" mode, we have obtained more than 40% of a total of 64 billion relations in the first phase (sieving). Some experiments were done together with an internship, Cyril Bouvier, for the filtering phase. The linear algebra phase is expected to finish by the end of 2009, or at the turn of the year. The linear algebra phase is considerably more challenging than the sieving phase in terms of program distribution. The block Wiedemann algorithm, which is being used for this computation, makes it possible to distribute the computation somewhat. Using Grid'5000 computers, we have been able to participate to a large extent to the linear algebra computation. The work on RSA-768 is expected to yield several forthcoming papers describing the many facets of the experiment.

Antoine Joux, Reynald Lercier, David Naccache and Emmanuel Thomé extended their work on oracle-assisted modular e-th root computation to an attack on the so-called static Diffie-Hellmann problem [10]. A revised version of this work has been accepted and presented at the 12th IMA workshop on cryptography and coding.

6.5. Hardware accelerators for pairing-based cryptography

Participants: Jérémie Detrey, Nicolas Estibals.

Together with J.-L. Beuchat, E. Okamoto (LCIS, University of Tsukuba, Japan), and F. Rodríguez-Henríquez (CINVESTAV, IPN, Mexico), J. Detrey and N. Estibals have proposed a new family of dedicated hardware coprocessors for computing the Tate pairing over supersingular elliptic curves in characteristic three. Designed following a performance-oriented rationale and based upon a fully parallel Karatsuba-like multiplier, these accelerators achieve the fastest computation speeds in the open literature (for instance, under 17μs for 109 bits of equivalent symmetric-key security). Moreover, due to a carefully controlled adequation between arithmetic, algorithms and architecture, these coprocessors also yield the best publicly-known area–time tradeoffs.

This work was published at the CHES 2009 conference [8], where it received a Best Paper Award. An extended version of this paper, also covering the case of characteristic two with further arithmetic and architectural advances, and similar or even better results than in characteristic three, was then submitted to a special issue of the IEEE Transactions on Computers [17].

N. Estibals has also developed a flexible compiler for a wide family of generic finite-field arithmetic coprocessors during his Master project [20]. This compiler will be extremely useful in automating the achitectural exploration of hardware pairing accelerators.

6.6. Symmetric cryptography

Participant: Marion Videau.

In October 2008, Marion Videau together with all the other 13 co-authors of the proposition submitted a new proposition called Shabal [22] to NIST's cryptographic Hash Algorithm Competition. The submission was accepted as a first round candidate in December 2008 and then as a secound round candidate in July 2009.

In September 2009, a common work with Andrea Röck (Helsinki University of Technology) and Vincent Strubel (ANSSI) on the Linux kernel random generator has been presented at *Journées C2* in Fréjus.

6.7. Legal aspects and security

Participant: Marion Videau.

In May 2009, Marion Videau made a presentation entitled "Aspects techniques de la preuve reposant sur l'écrit électronique" on the occasion of a symposium "La preuve des actes juridiques électroniques privés : mosaïque des droits européens ou trait d'Union", organized by the "Centre René DEMOGUE" of the "Faculté des Sciences Juridiques, Politiques et Sociales" of the University Lille 2. An article corresponding to its presentation has been published in [11].

In July 2009, Marion Videau also made a presentation and a poster entitled "Preliminary thoughts on national health identifier systems" on the occasion of the Young Engineering Scientist Symposium 2009 organized by the Office for Science and Technology (Ambassy of France, Washington DC).

6.8. Other results

S. Burckel, E. Gioan and E. Thomé wrote a paper on the computation of multi-dimensional mappings using a minimal number of intermediary registers. This paper has been presented at the UC 2009 conference [9].

7. Other Grants and Activities

7.1. National Initiatives

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

Participants: Cyril Bouvier, Pierrick Gaudry, Guillaume Hanrot, Alexander Kruppa, Lionel Muller, Emmanuel Thomé, Antonio Vera, 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. This grant has been running since November 2006, and ends in January 2010.

We worked on several aspects of this factoring algorithm, that are linked to our main objectives. Among other things, we investigated the so-called "polynomial selection" phase, we worked on the parallelization (in a Grid context) of the linear algebra step, we also studied the relation search phase, where the speed of the underlying arithmetic is crucial.

The most visible results are

- A complete implementation of the NFS algorithm: CADO-NFS (see the software section);
- The PhD thesis of A. Kruppa, to be defended in January 2010;
- The participation to the RSA-768 record computation (to be completed in December 2009 or January 2010).

7.1.2. ANR RAPIDE (Design and analysis of stream ciphers dedicated to constrained environments)

Participant: Marion Videau.

The project from "programme Sécurité Et Informatique 2006" involves the team together with the SECRET (former CODES) project-team, the XLIM lab from the university of Limoges and the CITI lab from INSA-Lyon. It has been running since January 2007 and will continue until the end of 2010.

The research project consists in the study and analysis, both from theoretical and practical points of view, of existing stream ciphers and new designs based on non-linear feedback shift registers.

Despite the departure of Marion Videau (on secondment to the cryptographic lab of the Agence Nationale de la Sécurité des Systèmes d'Information), the coordination tasks are held by her from the team side.

7.1.3. ANR DEMOTIS (Collaborative Analysis, Evaluation and Modelling of Health Information Technology)

Participant: Marion Videau.

The project from "programme ARPEGE" involves three INRIA project-teams as a single partner (SMIS, SECRET and CACAO) together with colleagues from CECOJI (CNRS) and the company Sopinspace. It has been running from January 2009 and will continue until the end of 2011.

The project experiments new methods for the multidisciplinary design of large information systems that have to take in account legal, social and technical constraints. Its main field of application is personal health information systems.

7.1.4. ANR CHIC (Courbes Hyperelliptiques, Isogénies, Comptage)

Participants: Pierrick Gaudry, Guillaume Hanrot, Emmanuel Thomé, Gaëtan Bisson, Romain Cosset, Damien Robert.

The team has obtained a financial support from the ANR ("programme blanc") for a project, common with colleagues from IRMAR (Rennes) and IML (Marseille). The principal investigator for this project is IRMAR. ANR CHIC has just begun in September 2009. The purpose of this ANR project is the study of several aspects of curves in genus 2, with a very strong focus on the computation of explicit isogenies between Jacobians.

7.2. International Initiatives

7.2.1. Collaboration with ANU

Participants: Shi Bai, Richard Brent, Judy-anne Osborn, Paul Zimmermann.

In the context of the "associate team" ANC (Algorithms, Numbers, Computers), which started in 2008 (http://www.loria.fr/~zimmerma/anc.html), between the CACAO project-team and the team of Richard Brent at the Australian National University (ANU), several visits were organized in 2009: R. Brent and J.-A. Osborn visited LORIA for two weeks in April-May, P. Zimmermann visited ANU for one month in July, and S. Bai visited LORIA for one month in October-November.

7.2.2. Collaboration with Tsukuba, Japan

Participants: Jérémie Detrey, Nicolas Estibals, Guillaume Hanrot.

In the context of the AYAME Junior Program on the subject of "Software and Hardware Components for Pairing-Based Cryptography" between the CACAO project-team, the Arénaire project-team and the Laboratory of Cryptography and Information Security (LCIS) of the University of Tsukuba (Japan), J.-L. Beuchat (Univ. Tsukuba) visited us for one week in February 2009. During this week, he worked with J. Detrey and N. Estibals to complete a paper for the CHES 2009 conference [8], for which they received a Best Paper Award. An extended version of this work was also submitted to the IEEE Transactions on Computers [17].

J.-L. Beuchat visited us again for one week in September 2009, along with T. Teruya, Ph.D. student at the University of Tsukuba. This visit was the occasion for us to continue working on the topic of pairings over genus-2 supersingular hyperelliptic curves. This work had been started during the visit of J. Detrey and G. Hanrot at Tsukuba in February 2008, and is now nearing completion.

7.2.3. Other visits

Part of an ongoing collaboration with F. Rodríguez-Henríquez, J. Detrey and N. Estibals spent three weeks in November 2009 at the CINVESTAV (*Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional*) in Mexico City. There, they continued their work on the automatic generation of finite-field multipliers, for use in hardware pairing coprocessors. J. Detrey also gave a twelve-hour course on pairings to the Master students of the CINVESTAV.

8. Dissemination

8.1. Scientific Animation

8.1.1. Cacao seminar

We have a seminar, where we have invited in 2009 the following speakers: Jean-Luc Beuchat, Nicolas Guillermin, Andy Novocin, Judy-Anne Osborn, Tadanori Teruya, Shi Bai, and Éric Brier.

8.1.2. Conference organization

Pierrick Gaudry and Emmanuel Thomé, together with Anne-Lise Charbonnier from the "comité colloques" of INRIA Nancy - Grand Est, are organizing the ANTS-IX conference[8], to be held at LORIA in July 2010. In 2009, the main part has been to search for sponsors and grants in order to prepare a budget. Jérémie Detrey designed the poster.

8.2. Committees memberships

P. Gaudry was a member in the "Comité de Sélection" for the hiring of an assistant Professor in Bordeaux (section 25). He was referee for the PhD thesis of Cédric Faure (École polytechnique and INRIA). He was a PC member of the PAIRING 2009 conference (Stanford, USA, August 2009) and of the INDOCRYPT 2009 conference (to be held in New Dehli, INDIA, December 2009).

M. Videau was a member of the program committee of the WCC'09 conference, which took place in Ullensvang (Norway) in May 2009. She was also a member of the program committee of the SSTIC'09 conference, which took place in Rennes (France) in June 2009.

P. Zimmermann is member of the program committee of the Arith'19 conference, which took place in Portland (Oregon) in June 2009. He was head in 2009 of the INRIA hiring committee for CR1 and CR2 at INRIA Nancy - Grand Est. He is also head of the "comité colloques" of INRIA Nancy - Grand Est, member of the "comité de liaison" of the new thematic group MAIRCI of the SMAI (Société de Mathématiques Appliquées et Industrielles), and was member of the PhD thesis committee of Guillaume Revy (ENS Lyon).

8.3. Vulgarization

- J. Detrey and P. Zimmermann participated once and twice, respectively, to the "*Une journée avec un scientifique*" program, where high-school students are invited to discover scientific research by spending a day among researchers, during which they are shown the various aspects of the job.
- P. Gaudry wrote an article about curves and cryptography, to be published, early 2010 in *Pour la science*.

8.4. Invited Conferences

P. Gaudry gave two one-hour invited talks at the "9th Central European Conference on Cryptography" in Třebíč, Czech Republic, and for the colloquium in the honor of Gerhard Frey for his retirement in Essen, Germany. He will give a 40-minute invited talk at the "Théorie des nombres et Applications" workshop, to be held at the CIRM center, Luminy, France, in December.

P. Zimmermann gave an invited talk at the 2nd public workshop of the SCIEnce Project in January (Paris, France), another one at Microsoft Research in June (Redmond, USA), and a third one at the *Rencontres "Arithmétique de l'Informatique Mathématique"* (RAIM'09) in October (Lyon, France).

E. Thomé gave an invited talk at the Sage Days 16 workshop in Barcelone (June).

J. Detrey gave an invited talk at the *Rencontres "Arithmétique de l'Informatique Mathématique"* (RAIM'09) in October (Lyon, France).

8.5. Teaching

- J. Detrey and G. Hanrot gave eight and twelve hours of lectures, respectively, at the *Master d'Informatique Fondamentale* of ENS Lyon, on the topic of elliptic curves and pairings applied to cryptography. They also sat in the examination jury for this course.
- J. Detrey gave a two-hour lecture in *licence professionnelle* at IUT Charlemagne (Nancy) on the topic of security.

[8] http://www.ants9.org/

- E. Thomé gave 8 hours of Master 1 courses at Université Henri Poincaré on the topic of cryptology and computer networks.
- E. Thomé is a member of the jury of the competitive exam for the École polytechnique.
- J. Detrey gave a twelve-hour course on the topic of pairings and pairing-based cryptography, as part of the Master in Computer Science of the CINVESTAV (Mexico City).
- P. Gaudry gave 30 hours of Master 1 courses at Université Henri Poincaré on the topic of cryptology.
- P. Gaudry and G. Hanrot are members of the jury of "agrégation externe de mathématiques", a competitive exam to hire high school teachers.
- J. Detrey supervised the Master 2 internship of Nicolas Estibals (ENS Lyon) on the topic of automatic compilation of arithmetic algorithms on families of finite-field coprocessors.
- P. Gaudry supervised the Master 1 internship of Răzvan Bărbulescu (ENS Lyon) on the topic of integer factorization using elliptic curves.
- P. Zimmermann supervised the Master 2 internship of Iram Chelli (Univ. Limoges) on the topic of a deterministic elliptic curve method.
- J. Detrey gave a three-hour lecture at the *Centre de formation à la sécurité des systèmes d'information* on the topic of discrete logarithm and elliptic curves.
- M. Videau gave 36 hours of lectures at the *Centre de formation à la sécurité des systèmes d'information* on cryptography.
- M. Videau gave 12 hours of lectures in cryptography at École Supérieure d'Informatique et Applications de Lorraine.
- M. Videau gave 26 hours of tutorials in algorithmic and programming at École Nationale Supérieure de Techniques Avancées.
- M. Videau gave a 2 hours seminar course on technical aspects of electronic proofs at the *Master Professionnel M2 - Spécialité Droit du Commerce Électronique et de l'Économie Numérique* of the University Paris I.

9. Bibliography

Major publications by the team in recent years

[1] R. P. BRENT, P. ZIMMERMANN. *Modern Computer Arithmetic*, Version 0.4, 2009, http://wwwmaths.anu.edu.au/~brent/pub/pub226.html, In preparation.

Year Publications

Articles in International Peer-Reviewed Journal

[2] R. P. BRENT, P. ZIMMERMANN. *Ten new primitive binary trinomials*, in "Mathematics of Computation", vol. 78, n^{o} 266, 2009, p. 1197-1199, http://hal.inria.fr/inria-00337525/en/.

[3] R. COSSET. *Factorization with genus 2 curves*, in "Mathematics of Computation", 2009, http://hal.inria.fr/inria-00384128/en/.

[4] M. DELÉGLISE, J.-L. NICOLAS, P. ZIMMERMANN. *Landau's function for one million billions*, in "Journal de Théorie des Nombres de Bordeaux", 2009, à paraître, http://hal.archives-ouvertes.fr/hal-00264057/en/.

[5] P. GAUDRY. *Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem*, in "Journal of Symbolic Computation", vol. 44, n^{o} 12, 2009, p. 1690-1702, http://hal.inria.fr/inria-00337631/en/.

[6] P. GAUDRY, D. LUBICZ. *The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines*, in "Finite Fields and Their Applications", vol. 15, n^{o} 2, 2009, p. 246-260, http://hal.inria.fr/inria-00266565/en/.

[7] S. RUMP, P. ZIMMERMANN, S. BOLDO, G. MELQUIOND. *Computing predecessor and successor in rounding to nearest*, in "BIT Numerical Mathematics", vol. 49, n^{o} 2, 2009, p. 419-431, http://hal.inria.fr/inria-00337537/en/DE.

International Peer-Reviewed Conference/Proceedings

[8] J.-L. BEUCHAT, J. DETREY, N. ESTIBALS, E. OKAMOTO, F. RODRÍGUEZ-HENRÍQUEZ. *Hardware Accelerator for the Tate Pairing in Characteristic Three Based on Karatsuba-Ofman Multipliers*, in "11th International Workshop on Cryptographic Hardware and Embedded Systems - CHES 2009, Suisse Lausanne", C. CLAVIER, K. GAJ (editors), vol. 5747, Springer, 2009, p. 225-239, http://hal.inria.fr/inria-00424011/en/MXJP.

[9] E. GIOAN, S. BURCKEL, E. THOMÉ. *Mapping Computation with No Memory*, in "8th International Conference on Unconventional Computation - UC09, Ponta Delgada, Portugal", Springer, 2009, 15, http://hal-lirmm.ccsd.cnrs.fr/lirmm-00395080/en/.

[10] A. JOUX, R. LERCIER, D. NACCACHE, E. THOMÉ. *Oracle-Assisted Static Diffie-Hellman Is Easier Than Discrete Logarithms*, in "Twelfth IMA International Conference on Cryptography and Coding, Cirencester Royaume-Uni", Lecture Notes in Computer Science, Springer, 2009, http://hal.inria.fr/inria-00337753/en/ UK.

National Peer-Reviewed Conference/Proceedings

[11] M. VIDEAU. *Aspects techniques de la preuve reposant sur l'écrit électronique*, in "La preuve des actes juridiques électroniques privés : mosaïque des droits européens ou trait d'Union ?, France Lille", Lamy, 2009, p. 15-18 (RLDI 1743), http://hal.archives-ouvertes.fr/hal-00432625/en/.

Scientific Books (or Scientific Book chapters)

[12] P. DUMAS, C. GOMEZ, B. SALVY, P. ZIMMERMANN. *Calcul formel : mode d'emploi. Exemples en Maple*, Version électronique, 2009, http://hal.inria.fr/inria-00371192/en/.

Research Reports

[13] E. BRESSON, A. CANTEAUT, B. CHEVALLIER-MAMES, C. CLAVIER, T. FUHR, A. GOUGET, T. ICART, J.-F. MISARSKY, M. NAYA-PLASENCIA, P. PAILLIER, T. PORNIN, J.-R. REINHARD, C. THUILLET, M. VIDEAU. *Indifferentiability with Distinguishers: Why Shabal Does Not Require Ideal Ciphers*, Cryptology ePrint Archive, 2009, http://eprint.iacr.org/2009/199, Technical report.

[14] I. CHELLI. *Fully deterministic ECM*, INRIA, 2009, http://hal.inria.fr/inria-00419083/en/, RR-7040, Rapport de recherche.

[15] A. KRUPPA. *A Software Implementation of ECM for NFS*, INRIA, 2009, http://hal.inria.fr/inria-00419094/en/, RR-7041, Rapport de recherche.

Other Publications

[16] R. BARBULESCU. *Familles de courbes adaptées à la factorisation des entiers*, 2009, http://hal.inria.fr/inria-00419218/en/, Internship report.

[17] J.-L. BEUCHAT, J. DETREY, N. ESTIBALS, E. OKAMOTO, F. RODRÍGUEZ-HENRÍQUEZ. *Fast Architectures for the η_T Pairing over Small-Characteristic Supersingular Elliptic Curves*, 2009, http://hal.inria.fr/inria-00424016/en/, Submitted at IEEE Transactions on ComputersMXJP.

[18] G. BISSON, A. V. SUTHERLAND. *Computing the endomorphism ring of an ordinary elliptic curve over a finite field*, 2009, http://hal.inria.fr/inria-00383155/en/, Accepted for publication in Journal of Number TheoryNLUS.

[19] A. ENGE, P. GAUDRY, E. THOMÉ. *An $L(1/3)$ Discrete Logarithm Algorithm for Low Degree Curves*, 2009, http://hal.inria.fr/inria-00383941/en/, Accepted for publication in Journal of Cryptology.

[20] N. ESTIBALS. *Génération automatique de circuits pour le calcul de couplages cryptographiques en matériel*, ENS Lyon, 2009, Masters thesis.

[21] J.-C. FAUGERE, D. LUBICZ, D. ROBERT. *Computing modular correspondences for abelian varieties*, 2009, http://hal.archives-ouvertes.fr/hal-00426338/fr/.

References in notes

[22] E. BRESSON, A. CANTEAUT, B. CHEVALLIER-MAMES, C. CLAVIER, T. FUHR, A. GOUGET, T. ICART, J.-F. MISARSKY, M. NAYA-PLASENCIA, P. PAILLIER, T. PORNIN, J.-R. REINHARD, C. THUILLET, M. VIDEAU. *Shabal, a Submission to NIST's Cryptographic Hash Algorithm Competition*, 2008, http://www.shabal.com/.

[23] 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.

[24] IEEE. *P1363: Standard specifications for public key cryptography*.

[25] N. KOBLITZ. *Elliptic curve cryptosystems*, in "Math. Comp.", n° 48, 1987, p. 203–209.

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

[27] 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.

[28] C. P. SCHNORR. *A Hierarchy of Polynomial Lattice Basis Reduction Algorithms*, in "Theoretical Computer Science", vol. 53, 1987, p. 201–224.

[29] M. SCOTT. *New record breaking implementations of ECC on quadratic extensions using endomorphisms*, September 2008, Invited talk at the ECC 2008 Conference. Utrecht, the Netherlands, Sep. 22-24, 2008..