INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team TANC

Théorie Algorithmique des Nombres pour la Cryptologie

Saclay - Île-de-France

THEME SYM

Table of contents

1. Team **1**
2. Overall Objectives **1**
2.1. Main topics 1
2.2. Exploratory topics 2
2.3. Highlights of the year 2
3. Scientific Foundations **2**
3.1. General overview 2
3.2. Algebraic curves over finite fields 3
3.2.1. Effective group laws 3
3.2.2. Cardinality 4
3.2.3. Computing isogenies 4
3.2.4. The discrete logarithm problem 5
3.2.5. Pairings on algebraic curves 5
3.3. Complex multiplication 5
3.3.1. Genus 1 5
3.3.2. Genus 2 6
3.4. Algebraic Geometry codes 7
4. Application Domains **7**
5. Software **7**
5.1. ECPP 7
5.2. mpc 7
5.3. mpfrcx 8
5.4. TIFA 8
6. New Results **9**
6.1. Algebraic curves over finite fields 9
6.1.1. Cardinality 9
6.1.2. Isogenies 9
6.1.3. Discrete logarithms on curves 10
6.2. Complex multiplication 10
6.3. Decoding algebraic codes 11
6.4. Security in ad hoc networks 11
7. Contracts and Grants with Industry **12**
7.1. Gemplus 12
7.2. Industrial ANR 12
8. Other Grants and Activities **12**
8.1. Network of excellence 12
8.2. ANR 12
8.3. Associated team 12
8.4. OMT 12
9. Dissemination **12**
9.1. Programme committees 12
9.2. Teaching 13
9.3. Seminars and talks 13
9.4. Vulgarisation and Summer schools 13
9.5. Editorship 14
9.6. Awards 14
9.7. Thesis committees 14
9.8. Research administration 14
10. Bibliography **14**

1. Team

Research Scientist

Andreas Enge [CR1, HdR]
Daniel Augot [CR1, HdR]
Ben Smith [CR2]

Faculty Member

François Morain [Professor at École polytechnique, HdR]

Technical Staff

Jérôme Milan [Ingénieur de Développement Digiteo]

PhD Student

Thomas Houtmann [CNRS/DGA until 2008-09-01]
Luca De Feo [École polytechnique since 2007-09-01]
Jean-François Biasse [DGA since 2007-09-01]
Morgan Barbier [École polytechnique since 2008-10-01]

Administrative Assistant

Évelyne Rayssac [École polytechnique]

2. Overall Objectives

2.1. Main topics

TANC *is located in the Laboratoire d'Informatique de l'École polytechnique (LIX). The project was created on 2003-03-10.*

The aim of the TANC project is to promote the study, implementation and use of robust and verifiable asymmetric cryptosystems based on algorithmic number theory.

It is clear from this statement that we combine high-level mathematics and efficient programming. Our main area of competence and interest is that of algebraic curves over finite fields, most notably the computational aspects of these objects, that appear as a substitute of good old-fashioned cryptography based on modular arithmetic. One of the reasons for this change is that the key-size is much smaller for an equivalent security. We participate in the recent bio-diversity mood that tries to find substitutes for old-fashioned cryptosystems as the very famous RSA system (for Rivest/Shamir/Adleman), in case some attack would appear and destroy the products that employ it.

Whenever possible, we produce certificates (proofs) of validity for the objects and systems we build. For instance, an elliptic curve has many invariants, and their values need to be proved, since they may be difficult to compute.

Our research area includes:

- Fundamental number theoretic algorithms: we are interested in primality proving algorithms based on elliptic curves, integer factorization, and the computation of discrete logarithms over finite fields. These problems lie at the heart of the security of arithmetic based cryptosystems.
- Algebraic curves over finite fields: the algorithmic problems that we tackle deal with the efficient computation of group laws on Jacobians of curves, evaluation of the cardinality of these objects, and the study of the security of the discrete logarithm problem in such groups. These topics are the crucial problems to be solved for potential use in real crypto-products.
- Complex multiplication: the theory of complex multiplication is a meeting point of algebra, complex analysis and algebraic geometry. Its applications range from primality proving to the efficient construction of elliptic and hyperelliptic curve-based cryptosystems.

- Pairings: The new number theoretic primitive of pairings (i.e. bilinear functions) on algebraic curves enables many novel applications, and poses algorithmic challenges concerning efficient implementation and the creation of secure instances.
- Decoding algorithms for Algebraic Geometric codes. The algorithmic knowledge of TANC will be used to accelerate the decoding algorithms, be they the classical one (up to half to the minimum distance), or new ones, which decode many more errors.

2.2. Exploratory topics

As described in the name of our project, we aim to provide robust primitives for asymmetric cryptography. In recent years, we have made several attempts at applying our knowledge to real life protocols. We are currently trying to promote the use of elliptic curves in environments where they could be useful, such as *ad hoc* networks. We will also try to promote the use of AG codes, which are to coding theory what elliptic curve cryptography is to cryptology.

2.3. Highlights of the year

B. Smith won the Best Paper award at EUROCRYPT 2008, the premier European conference in cryptology, for his work on discrete logarithms in genus 3 [18].

A. Enge has won the Selfridge Prize of the Number Theory Foundation for the best paper [17] presented at ANTS-VIII in Banff, the main, biennial conference for algorithmic number theory.

The team organized the C4 (Computations on Curves for Crypto and Coding) workshop, held on the 9th and 10th of June 2008 at the École polytechnique, bringing together leading researchers from France, the United States, Canada, Denmark, and the Netherlands.

The team has contributed to the organisation of the CADO Workshop on Integer Factorization, held jointly with the CACAO project team in Nancy [19].

3. Scientific Foundations

3.1. General overview

Keywords: *Cryptology*, *arithmetic*.

Once considered beautiful but useless, arithmetic has proven incredibly efficient when asked to assist the creation of a new paradigm in cryptography. Classical cryptography was mainly concerned with *symmetric techniques*: two principals wishing to communicate secretly had to share a common secret beforehand and this same secret was used both for encrypting the message and for decrypting it. This way of communication is efficient enough when traffic is low, or when the principals can meet prior to communication.

It is clear that modern networks are too large for this to remain efficient any longer. Hence the need for cryptography without first contact. In theory, this is easy. Find two algorithms E and D that are reciprocal (i.e., $D(E(m)) = m$) and such that the knowledge of E does not help in computing D. Then E is dubbed a public key available to anyone, and D is the secret key, reserved to a user. When Alice wants to send an email to Bob, she uses his public key and can send him the encrypted message, without agreeing on a common key beforehand. Though simplified and somewhat idealized, this is the heart of asymmetric cryptology. Apart from confidentiality, modern cryptography provides good solutions to the signature problem, as well as some solutions for identifying all parties in protocols, thus enabling products to be usable on the INTERNET (ssh, ssl/tls, etc.).

Of course, everything has to be presented in the modern language of complexity theory: E and D must be computable in polynomial time; finding D from E alone should be possible only in, say, exponential time, without some secret knowledge.

Now, where do difficult problems come from? Mostly from arithmetic, where we find problems such as the integer factorization problem and the discrete logarithm problem. Varying the groups appears to be important, since this provides some bio-diversity which is the key of the resistance to attacks from crypto-analysts. Among the groups proposed: finite fields, modular integers, algebraic curves, class groups, etc. All these now form cryptographic primitives that need to be assembled in protocols, and finally in commercial products.

Our activity is concerned with the beginning of this process: we are interested in difficult problems arising in computational number theory and the efficient construction of these primitives. TANC concentrates on modular arithmetic, finite fields and algebraic curves.

We have a strong well-known reputation of breaking records whatever the subject is: constructing systems or breaking them, including primality proving, class polynomials, modular equations, computing cardinalities of algebraic curves, discrete logs, etc. This means writing programs and putting in all the work needed to make them run for weeks or months. An important part of our task is now to transform record programs into ones that can solve everyday life problems for current sizes of the parameters.

Efficiency is not our single concern. Certificates are again another one. By this, we mean that we provide proofs of the properties of the objects we build. The traditional example is that of prime numbers, where certificates were introduced by Pratt in 1974. These certificates might be difficult to build, yet they are easy to check (by customers, say). We know how to do this for elliptic curves, with the aim of establishing what we call an **identity card** for a curve, including its cardinality together with the proof of its factorization, its group structure (with proven generators), discriminant (and factorization), and class number of the associated order. The theory is ready for this, algorithms not out of reach. This must be extended to other curves, and in several cases, the theory is almost ready or not at all, and algorithms still to be found. This is one of the main problems we have to tackle in TANC.

It is clear that more and more complex mathematics will be used in cryptology (see the recent algorithms that use p-adic approaches). These cannot live if we do not implement them, and this is where we need more and more evolved algorithms, that are for the moment present in very rare mathematical systems, like MAGMA that we use for this. Once the algorithms work in MAGMA, it is customary to rewrite them in C or C++ to gain speed. Along the same lines, some of our C programs developped for our research (an old version of ECPP, some parts of discrete log computations, cardinality of curves) are now included in this system, as a result of our collaboration with the Sydney group.

3.2. Algebraic curves over finite fields

One of the most used protocols is that of Diffie-Hellman that enables Alice and Bob to exchange a secret information over an insecure channel. Given a publicly known cyclic group G of generator g, Alice sends g^a for a random a to Bob, and Bob responds with a random g^b. Both Alice and Bob can now compute g^{ab} and this is henceforth their common secret. Of course, this a schematic presentation, since real-life protocols based on this need more security properties. Being unable to recover a from g^a (the discrete log problem – *DLP*) is a major concern for the security of the scheme, and groups for which the *DLP* is difficult must be favored. Therefore, groups are important, and TANC concentrates on algebraic curves, since they offer a very interesting alternative to finite fields, in which the *DLP* can be broken by subexponential algorithms, whereas exponential time is required for curves. Thus a smaller key can be used using curves, and this is very interesting as far as limited powered devices are concerned.

In order to build a cryptosystem based on an algebraic curve over a finite field, one needs to efficiently compute the group law (hence have a nice representation of the elements of the Jacobian of the curve). Next, computing the cardinality of the Jacobian is required, so that we can find generators of the group. Once the curve is built, one needs to test its security, for example how hard the discrete logarithm in this group is.

3.2.1. Effective group laws

A curve that interests us is typically defined over a finite field $\mathrm{GF}(p^n)$, where p is the characteristic of the field.

The points of an elliptic curve E (of equation $y^2 = x^3 + ax + b$, say) form an abelian group, that was thoroughly studied during the preceding millenium. Adding two points is usually done using the so-called *chord-and-tangent* formulæ. When dealing with a genus g curve (the elliptic case being $g = 1$), the associated group is the Jacobian (set of g-tuples of points modulo an equivalence relation), an object of dimension g. Points are replaced by polynomial ideals. This requires the help of tools from effective commutative algebra, such as Gröbner bases or Hermite normal forms.

The great catalog of usable curves is now complete, as a result of the work of TANC, notably in two ACI (CRYPTOCOURBES and CRYPTOLOGIE P-ADIQUE) that are finished now.

3.2.2. Cardinality

Once the group law is tractable, one has to find means of computing the cardinality of the group, which is not an easy task in general. Of course, this has to be done as fast as possible, if changing the group very frequently in applications is imperative.

Two parameters enter the scene: the genus g of the curve, and the characteristic p of the underlying finite field. When $g = 1$ and p is large, the only current known algorithm for computing the number of points of $E/\mathrm{GF}(p)$ is that of Schoof–Elkies–Atkin. Thanks to the works of the project, world-widespread implementations are able to build cryptographically strong curves in less than one minute on a standard PC. Recent improvements were made by F. Morain and P. Gaudry (CACAO), see [42]. The current record of SEA was established by F. Morain in 2007 for a prime p of 2500 decimal digits (again compared to 500dd back in 1995), using the work in [10] (see below), as well as [6], in which a new approach to the eigenvalue computation is described and proven.

When p is small (one of the most interesting cases for hardware implementation in smart cards being $p = 2$) the best current methods use p-adic numbers, following the breakthrough of T. Satoh with a method working for $p \geq 5$. The first version of this algorithm for $p = 2$ was proposed independently by M. Fouquet, P. Gaudry and R. Harley and by B. Skjernaa. J. -F. Mestre has designed the currently fastest algorithm using the arithmetico-geometric mean (AGM) approach. Developed by R. Harley and P. Gaudry, it led to new world records. Then, P. Gaudry combined this method together with other approaches, to make it competitive for cryptographic sizes [41].

When $g > 1$ and p is large, polynomial time algorithms exist, but their implementation is not an easy task. P. Gaudry and É. Schost have modified the best existing algorithm so as to make it more efficient. They were able to build the first random cryptographically strong genus 2 curves defined over a large prime field [43]. To get one step further, one needs to use genus 2 analogues of modular equations. After a theoretical study [44], they are now investigating the practical use of these equations.

When $p = 2$, p-adic algorithms led to striking new results. First, the AGM approach extends to the case $g = 2$ and is competitive in practice (only three times slower than in the case $g = 1$). In another direction, Kedlaya has introduced a new approach, based on the Monsky-Washnitzer cohomology. His algorithm works originally when $p > 2$. P. Gaudry and N. Gürel implemented this algorithm and extended it to superelliptic curves, which had the effect of adding these curves to the list of those usable in cryptography.

Closing the gap between small and large characteristic leads to pushing the p-adic methods as far as possible. In this spirit, P. Gaudry and N. Gürel have adapted Kedlaya's algorithm and exhibited a linear complexity in p, making it possible to reach a characteristic of around 1000 (see [39]). For larger p's, one can use the Cartier-Manin operator. Recently, A. Bostan, P. Gaudry and É. Schost have found a much faster algorithm than currently known ones [25]. Primes p around 10^9 are now doable.

3.2.3. Computing isogenies

The core of the Schoof-Elkies-Atkin (SEA) algorithm that computes the cardinality of elliptic curves over finite fields consists in using the theory of isogenies to find small factors of division polynomials. SEA is still the method of choice for the large characteristic case, but no longer for small characteristics.

Isogenies are also a tool for understanding the difficulty of the Discrete Log problem among classes of elliptic curves [51]. Recently, there appeared suggestions to use isogenies in a cryptographic context, replacing the multiplication on curves by the use of such morphisms [62], [59].

Algorithms for computing isogenies are very well known and used in the large characteristic case. When the characteristic is small, three algorithms exist: two of these are due to Couveignes [29], [30], [55] and one to Lercier [54].

3.2.4. The discrete logarithm problem

The discrete logarithm problem is one of the major difficult problems that allow to build secure cryptosystems. It has essentially been proved equivalent to the computational Diffie–Hellman problem, which is closer to the actual security of many systems. For an arbitrary group of prime order N, it can be solved by a generic, exponential algorithm using $\Theta(\sqrt{N})$ group operations. For elliptic curves, set aside some rare and easily avoidable instances, no faster algorithms are known.

In higher genus curves, the algorithms with the best complexity create relations as smooth principal divisors on the curve and use linear algebra to deduce discrete logarithms, similarly to the quadratic sieve for factoring. The first such algorithm for high genus hyperelliptic curves with a heuristic complexity analysis is given in [21], and A. Enge has developed the first algorithm with a proven subexponential run time of $L(1/2)$ in [35]. Generalisations to further groups suggested for cryptography, in particular ideal class groups of imaginary quadratic number fields, are obtained by A. Enge and P. Gaudry in [2] [34]. Proofs for arbitrary curves of large genus are given by J.-M. Couveignes [28] and F. Heß [49].

The existence of subexponential algorithms shows that high genus curves are less secure than, say, elliptic ones in cryptography. By analysing the same algorithms differently, concrete recommendations for key lengths can be obtained, an approach introduced by P. Gaudry in [40] and pursued in [45]. It turns out that elliptic curves and hyperelliptic curves of genus 2 are not affected, while the key lengths have to be increased in higher genus, for instance by 12 % in genus 3.

Using similar algorithms to those analysed in [2], C. Diem has shown in [31] that non-hyperelliptic curves (of genus at least 3) are even less secure than hyperelliptic ones of the same genus. This effectively leaves elliptic and low genus hyperelliptic curves as potential sources for public-key cryptosystems.

3.2.5. Pairings on algebraic curves

Algebraic curves have first been used in cryptography as a source for groups in which the discrete logarithm problem should be harder than in the multiplicative group of a finite field. Totally new applications stem from the use of structures proper to algebraic curves, the Tate and Weil pairings. These are bilinear maps that associate to two group elements, at least one of which is defined in an extension field, a root of unity in the same extension field. Among the first new cryptographic primitives were a tripartite Diffie–Hellman key exchange [52] and identity based encryption [60]. Subsequently, the number of articles concerned with pairings has exploded, and a specialised series of conferences has been inaugurated with Pairings 2007 in Tokyo, A. Enge being a member of the programme committees in 2007 and 2008.

One of the most challenging problems related to pairing based cryptography is to find suitable curves, that are hidden like needles in a hay stack. Supersingular elliptic curves yield a rather limited supply of doubtful security. Using its expertise on complex multiplication, the TANC team has published one of the first two algorithms for finding pairing friendly ordinary curves for arbitrary field extension degrees in [33], the other one being developed in [22].

3.3. Complex multiplication

3.3.1. Genus 1

Despite the achievements described above, random curves are sometimes difficult to use, since their cardinality is not easy to compute or useful instances are too rare to occur (curves for pairings for instance). In some cases, curves with special properties can be used. For instance curves with *complex multiplication* (in brief

CM), whose cardinalities are easy to compute. For example, the elliptic curve defined over $GF(p)$ of equation $y^2 = x^3 + x$ has cardinality $p + 1 - 2u$, when $p = u^2 + v^2$, and computing u is easy.

The CM theory for genus 1 is well known and dates back to the middle of the nineteenth century (Kronecker, Weber, etc.). Its algorithmic part is also well understood, and recently more work was done, largely by TANC. Twenty years ago, this theory was applied by Atkin to the primality proving of arbitrary integers, yielding the ECPP algorithm developed ever since by F. Morain. Though the decision problem ISPRIME? was shown to be in *P* (by the 2002 work of Agrawal, Kayal, Saxena), practical primality proving of large random numbers is still done only with ECPP.

These CM curves enabled A. Enge, R. Dupont and F. Morain to give an algorithm for building good curves that can be used in identity based cryptosystems [33].

CM curves are defined by algebraic integers, whose minimal polynomials have to be computed exactly, the coefficients being exact integers. The fastest algorithm to perform these computations requires a floating point evaluation of the roots of the polynomial to a high precision. F. Morain on the one hand and A. Enge (together with R. Schertz) on the other, have developed the use of new class invariants that characterize CM curves. The union of these two families is currently the best that can be achieved in the field (see [4]). Later, F. Morain and A. Enge have designed a fast method for the computation of the roots of this polynomial over a finite field using Galois theory [36]. These invariants, together with this new algorithm, are incorporated in the working version of the program ECPP.

F. Morain analyzed a fast variant of ECPP, called fastECPP, which led him to gain one order of magnitude in the complexity of the problem (see [9] [57]), reaching heuristically $O((\log N)^{4+\epsilon})$, compared to $O((\log N)^{5+\epsilon})$ for the basic version. By comparison, the best proven version of AKS [53] has complexity $O((\log N)^{6+\epsilon})$ and has not been implemented so far; the best randomized version [23] reaches the same $O((\log N)^{4+\epsilon})$ bound but suffers from memory problems and is not competitive yet. F. Morain implemented fastECPP and was able to prove the primality of $10,000$ decimal digit numbers [9], as opposed to $5,000$ for the basic (historical) version. Continuously improving this algorithm, this led to new records in primality proving, some of which obtained with his co-authors J. Franke, T. Kleinjung and T. Wirth [38] who developed their own programs. F. Morain set the current world record to 20,562 decimal digits early June 2006, as opposed to 15,071 two years before. This record was made possible by using an updated MPI-based implementation of the algorithm and its distribution process on a cluster of 64-bit bi-processors (AMD Opteron(tm) Processor 250 at 2.39 GHz). In 2007, another large number was proven to be prime, namely $(2^{42737} + 1)/3$ with $12,865$ decimal digits.

In his thesis, R. Dupont has investigated the complexity of the evaluation of some modular functions and forms (such as the elliptic modular function j or the Dedekind eta function for example). High precision evaluation of such functions is at the core of algorithms to compute class polynomials (used in complex multiplication) or modular polynomials (used in the SEA elliptic curve point counting algorithm).

Exploiting the deep connection between the arithmetic-geometric mean (AGM) and a special kind of modular forms known as theta constants, he devised an algorithm based on Newton iterations and the AGM that has quasi-optimal linear complexity. In order to certify the correctness of the result to a specified precision, a fine analysis of the algorithm and its complexity was necessary [11].

Using similar techniques, he has given a proven algorithm for the evaluation of the logarithm of complex numbers with quasi-optimal time complexity.

3.3.2. Genus 2

The theory of Complex Multiplication also exists for non-elliptic curves, but is more intricate, and only recently can we dream to use them. Some of the recent results occurred as the work of R. Dupont (former member of TANC) in his thesis.

R. Dupont has worked on adapting his algorithm to genus 2, which induces great theoretical and technical difficulties. He has studied a generalization of the AGM known as Borchardt sequences, has proven the convergence of these sequences in a general setting, and has determined the set of limits such sequences have in genus 2. He has then developped an algorithm for the fast evaluation of theta constants in genus 2, and

as a byproduct obtains an algorithm to compute the Riemann matrix of a given hyperelliptic curve: given the equation of such a curve, it computes a lattice L such that the Jacobian of the curve is isomorphic to $\mathbb{C}/L$. These algorithms are both quasi-linear, and have been implemented (in C, using the multiprecision package GMP – see http://gmplib.org/).

Using these implementations, R. Dupont has began computing modular polynomials for groups of the form $\Gamma_0(p)$ in genus 2 (these polynomials link the genus 2 j-invariants of p-isogenous curves). He computed the modular polynomials for $p = 2$, which had never been done before, and did some partial computations for $p = 3$ (results are available at http://www.lix.polytechnique.fr/Labo/Regis.Dupont).

He also studied more theoretically the main ingredient used in his algorithms in genus 2, a procedure known as Borchardt sequences. In particular, he proved a theorem that parametrizes the set of all possible limits of Borchardt sequences starting with a fixed 4-tuple.

3.4. Algebraic Geometry codes

There are many other applications of algorithmic methods on algebraic curves than simple cryptography. Daniel Augot plans to develop a new activity around algebraic geometry codes, in short AG codes, which are a very powerful family of codes, who often beat records on their parameters: they often offer the best correction capacity. The main topics of research is to accelerate the decoding algorithms of these codes, who have a slightly expensive cost [50]. A reference implementation would be of major interest, to help people comparing these codes with the Reed-Solomon codes.

A breakthrought has been obtained by Guruswami and Sudan [47] for decoding these codes with many errors. Still, yet no implementation is avalaible, even for the most simple AG codes, which are the Hermitian codes. In this domain too, an objective is to produce a publicly available reference implementation.

4. Application Domains

4.1. Telecom

Our main field of applications is clearly that of telecommunications. We participate in the protection of information. We are proficient on a theoretical level, as well as ready to develop applications using modern cryptologic techniques, with a main focus on elliptic curve cryptography. One potential application are cryptosystems in environments with limited resources as smart cards, mobile phones or *ad hoc* networks.

5. Software

5.1. ECPP

F. Morain has been continuously improving his primality proving algorithm called ECPP, originally developed in the early '90. Binaries for version 6.4.5 are available since 2001 on his web page. Proving the primality of a 512 bit number requires less than a second on a GHz PC. His personal record is about $20,000$ decimal digits, with the fast version he started developing in 2003. Everything there is written in C, based on the GMP package.

5.2. mpc

The `mpc` library, developed in C by A. Enge in collaboration with Ph. Théveny and P. Zimmermann, implements the basic operations on complex numbers in arbitrary precision, which can be tuned to the bit. This library is based on the multiprecision libraries GMP and `mpfr`. Each operation has a precise semantics, in such a way that the results do not depend on the underlying architecture. Several rounding modes are available. This software, licensed under the GNU Lesser General Public License (LGPL), can be downloaded freely from the URL http://www.multiprecision.org/mpc/.

The library currently benefits from an Opération de développement logiciel of INRIA. The latest version 0.5 has been released in September 2008. A Debian package is available in the unstable distribution since October 2008. The perl wrapper Math::MPC (http://search.cpan.org/~sisyphus/Math-MPC/) is available on CPAN since version 0.4.6.

The `mpc` library is used in our team to build curves with complex multiplication and to compute modular polynomials (cf. Section 6.1), and it is *de facto* incorporated in the ECPP program. It is used by the Magma Computational Algebra System (http://magma.maths.usyd.edu.au/magma/) and by Trip (http://www.imcce.fr/Equipes/ASD/trip/trip.php), a symbolic-numeric system for celestial mechanics developed at Institut de Mécanique Céleste et de Calcul des Éphémérides

5.3. mpfrcx

The `mpfrcx` library is developed in C by A. Enge to implement the arithmetic of univariate polynomials with floating point coefficients of arbitrary precision, be they real (`mpfr`) or complex (`mpc`). The first version 0.1, published in October 2007 and available at http://www.lix.polytechnique.fr/Labo/Andreas.Enge/Software.html, contains the functionality needed for the author's complex multiplication program. Advanced asymptotically fast algorithms have been implemented, such as Karatsuba and Toom–Cook multiplication, various flavours of the FFT and division with remainder by Newton iterations. Special algorithms of symbolic computation such as fast multievaluation are also available.

Publishing `mpfrcx` is part of an ongoing effort to make A. Enge's program for building elliptic curves with complex multiplication available. This program is a very important building block for cryptographic purposes as well as for primality proving (fastECPP).

5.4. TIFA

We have hired J. Milan as *ingénieur associé* to help us with our programs. He first spent some time making a tour of publicly available platforms implementing the IEEE P-1363 cryptography standards. Following this work, it appeared not interesting to add a new one to the list, and he switched to one of our other themes, namely writing integer factorization software for which the results can be guaranteed.

However, besides this quite daunting task, we have a more pragmatic, twofold-interest in fast factorization implementations for small numbers.

- Our first motivation is directly related to the ANR CADO project [19] we are involved in, together with other teams such as the INRIA project-team CACAO. The objective of the CADO project is to implement an optimized and distributed implementation of the Number Field Sieve (NFS), asymptotically the fastest integer factorization algorithm currently known. This algorithm needs to factor a lot of much smaller integers (about 80 bits for current factorization records). Since a recursive application of the NFS would be totally inefficient in practice, there is indeed a need for routines better suited to factor this wealth of smaller by-products.
- Our second motivation lies in our long-term commitment to produce identity cards for elliptic curves in order to select those curves with the needed properties for cryptographic use. Such an identification would require the knowledge of the factorization of the order of the curve (about 200 bits for cryptographic use).

Hence, J. Milan is still actively developing the so-called TIFA library (short for Tools for Integer FActorization). TIFA is made up of a base library written in C99 and using the GMP library, together with stand-alone factorization programs and a basic benchmarking framework to assess the performance of the relative algorithms.

During the past year, TIFA has gone through a significant code refactoring aimed at facilitating its extensibility. Aside from optimizations made to the base library, several factorization algorithms were also added. As of september 2007, the following algorithms have been implemented:

CFRAC	(Continued FRACtion factorization [58])
ECM	(Elliptic Curve Method)
Fermat	(McKee's "fast" variant of Fermat's algorithm [56])
QS	(Quadratic Sieve [27])
SIQS	(Self-Initializing Quadratic Sieve [27])
SQUFOF	(SQUare FOrm Factorization [46])

In particular, a significant effort was made to fine tune the SQUFOF implementation for small (at most) double-precision numbers. We believe that TIFA's SQUFOF is quite competitive compared to other similar implementations, even if in practice, SQUFOF is rapidly outperformed by TIFA's QS. Our implementations of QS and SIQS have been substancially revamped in late 2007/early 2008. While still slightly slower then the best available implementations, the performance gap has been dramatically narrowe. An implementation of ECM has been added to TIFA in late 2007. However its performance is far from being on par with the competition. We hope to address these shortcomings – if time permits – in the near future.

While still kept internal to the TANC team and CADO project, TIFA will eventually be made public under an open source license, most probably the Lesser General Public License version 2.1 or higher.

6. New Results

6.1. Algebraic curves over finite fields

6.1.1. Cardinality

Participants: Andreas Enge, François Morain.

A crucial ingredient for these records was A. Enge's new algorithm [12] for computing modular equations of index greater than 2000. The algorithm computes bivariate modular polynomials by an evaluation and interpolation approach and relies on the ability to rapidly evaluate modular functions in complex floating point arguments. It has a quasi-linear complexity with respect to its output size, so that the performance of the algorithm is limited only by the size of the result: we have in fact been able to compute modular polynomials of degree larger than 10000 and of size 16 GB by a parallelised implementation of the algorithm, that uses `mpc` and `mpfrcx` for the arithmetic of complex numbers and of polynomials with floating point coefficients, see Sections 5.2 and 5.3. For the point counting algorithm, the polynomials of prime level up to 6000 have been used. They occupy a disk space of close to 1 TB. Despite this progress, computing modular polynomials remains the stumbling block for new point counting records. Clearly, to circumvent the memory problems, one would need an algorithm that directly obtains the polynomial specialised in one variable.

We plan to make our new implementation available as an extension to the NTL library.

6.1.2. Isogenies

Participants: François Morain, Luca De Feo.

Together with A. Bostan, B. Salvy (from projet ALGO), and É. Schost, F. Morain gave quasi-linear algorithms for computing the explicit form of a strict isogeny between two elliptic curves, another important block in the SEA algorithm [10]. This article contains a survey of previous methods, all applicable in the large characteristic case. Joux and Lercier have recently announced a p-adic approach for computing isogenies in all characteristic with the same complexity and based on our work.

For the small case, the old algorithms of Couveignes and Lercier were studied from scratch, and Lercier's algorithm reimplemented in NTL by F. Morain, as a benchmark for other methods still being developped. In his master internship, L. De Feo, started cleaning the most recent of them, known as CouveignesII. This algorithm involves building the explicit p^k torsion of the curve and finding isomorphisms between Artin-Schreier towers. This work already led to the clarification of the complexities involved in several parts. Ongoing work with É. Schost already led to improved theoretical constructions and faster algorithms. Several articles are in preparation as a result of a long term visit of De Feo in London (Ontario). A fresh implementation in NTL will follow.

6.1.3. Discrete logarithms on curves

Participants: Andreas Enge, Jean-François Biasse, Benjamin Smith.

In 2007 for the very first time in algebraic curve cryptography, A. Enge and P. Gaudry have exhibited a class of curves in which the discrete logarithm problem is attacked by a subexponential algorithm of complexity less than $L(1/2)$ [3]. Precisely, the complexity is in $L(1/3)$ for the preliminary phase of computing the group structure and $L(1/3+\varepsilon)$ for any $\varepsilon > 0$ for the discrete logarithms themselves. This shows that the corresponding algebraic curve cryptosystems, essentially based on $C_{a,b}$ curves with the degrees in X and Y growing in a special way with the genus, are no more secure than RSA and thus of no cryptographic interest.

This year, we have been able to extend the attack to a much larger class of curves, not necessarily of $C_{a,b}$ type, for which the degrees in X and Y grow in a controlled way. We have removed the ε for the discrete logarithm phase, and have come up with a tight complexity analysis that explains the phase change between the $L(1/3)$ and the $L(1/2)$ zone. A publication is in preparation.

Jean-François Biasse has worked on an implementation of a subexponential algorithm which solves the discrete logarithm problem on hyperelliptic curves of genus 8 in order to study the efficiency of a cryptosystem that Edlyn Teske has presented. This cryptosystem relies on the facility of solving this problem, as well as the difficulty of solving the discrete logarithm problem on an elliptic curve. This work was presented in October 2008 at the "Journée Nationales du Calcul Formel" in Luminy.

In another direction, B. Smith has given a polynomial-time reduction of discrete logarithm problem instances from a large class of hyperelliptic curves of genus 3 to non-hyperelliptic curves of genus 3, where Diem's algorithm [31] can solve the discrete logarithm problem in time $O(q)$. This is a significant improvement over the previous best known algorithm for solving hyperelliptic genus 3 discrete logarithms, due to P. Gaudry, E. Thomé, N. Thériault, and C. Diem [45], which runs in time $O(q^{4/3})$.

6.2. Complex multiplication

Participants: Andreas Enge, François Morain.

A. Enge has been able to analyse precisely the complexity of class polynomial computations via complex floating point approximations [13]. Using techniques from fast symbolic computation, namely multievaluation of polynomials, and results from R. Dupont's PhD thesis [32], he has obtained two algorithms which are quasi-linear (up to logarithmic factors) in the output size. The second algorithm has been used for a record computation of a class polynomial of degree 100,000, the largest coefficient of which has almost 250,000 bits. The implementation is based on GMP, mpfr, mpc and mpfrcx (see Section 5); the only limiting factor for going further has become the memory requirements of the final result.

Alternative algorithms use p-adic approximations or the Chinese remainder theorem to compute class polynomials over the integers. A. Enge and his coauthors have presented an optimised algorithm based on Chinese remaindering in [17] and improved the number theoretic bounds underlying the complexity analysis. They have shown that all three different approaches have a quasi-linear complexity, while the the floating point algorithm appeared to be the fastest one in practice.

Inspired by [17], A. Sutherland has come up with a new implementation of the Chinese remainder based algorithm that has led to new record computations [61]. Unlike the other algorithms, this approach does not need to hold the complete polynomial in main memory, but essentially only one coefficient at a time, which enables it to go much further. The main bottleneck is currently an extension of the algorithm to class invariants, which is work in progress by A. Enge.

6.3. Decoding algebraic codes

Participants: Daniel Augot, Morgan Barbier.

This is a new activity of the TANC project-team, whose aim is to accelerate decoding algorithms of Reed-Solomon codes (with the Guruswami-Sudan algorithm), and of Algebraic Geometric codes. With Alexander Zeh, Daniel has found a relation between so-called key equations, which are the standard tool for decoding algebraic codes, and the new interpolation based algorithms [16]. The connection is established, and the next step is to use efficient algorithms, that are used for key equations, in the context of the Guruswami-Sudan algorithm.

Another new topic that begins with the arrival of Morgan Barbier is to study list decoding algorithms for codes defined over small alphabets. It was a challenging open problem until the publication of Wu [63], which achieves a high decoding radius for BCH codes, which are subfield subcodes of Reed-Solomon codes. This opens a new field of applications of these algorithms, and we have in mind to apply Wu's algorithm for steganography, using the ideas of Fontaine and Galand [37]. They used Reed-Solomon codes, it seems very natural to use the same ideas with BCH codes. Providing an implementation of Wu's algorithm and apply it to steganography is the plan of Barbier's thesis.

6.4. Security in ad hoc networks

Participants: François Morain, Daniel Augot, Jérôme Milan.

As we mentioned in our previous activity reports, we saw the recent arrival of HIPERCOM at École polytechnique as an opportunity to trigger inter-project collaborations in the field of security and cryptographic applications in the context of ad hoc networks.

Following upon our involvement in the ACI SERAC (SEcuRity models and protocols for Ad-hoC Networks) a short one-year teamwork between TANC and HIPERCOM@LIX was initiated in January 2008 as part of the so-called Cryptonet OMT (Opération de Maturation Technologique). This joint effort is mainly financed by the Digiteo foundation who hired J. Milan to work as a software programmer and provides marketing and intellectual property legal assistance.

The main goal of Cryptonet is to present a proof-of-concept of an hardened, more robust OLSRv2 [26] ad hoc network protocol. For this, we are working with Thomas Clausen and Ulrich Herberg from the HIPERCOM@LIX team to bring some basic authentification mechanism in OLSRv2 using digital signature based on elliptic curves (ECDSA [20] and pairings on such curves (BSL-like signature [24]).

Such a mechanism has been developped and integrated within HIPERCOM@LIX's jOlsrv2 [48] framework which provides a Java-based implementation of the OLSRv2 protocol and interfaces with the NS2 network simulator.

Of course achieving ad hoc network security requires far more than mere application of cryptographic primitives. However, by presenting a first milestone, our goal is to spread awareness on major security issues arising in the mobile ad hoc network context. We hope to attract industrial partners with a practical stance on security and ultimately foster new academic-industrial partnerships.

Daniel Augot, in cooperation with Hipercom, has worked on Group Key Agreement Protocols, generalizing the Diffie-Hellman protocol. ALthought the theoretical part has been published, a new paper with simulation results is in preparation.

7. Contracts and Grants with Industry

7.1. Gemplus

This corresponds to É. Brier's thesis on the use of (hyper-)elliptic curves in cryptology.

7.2. Industrial ANR

PACE: Pairings and advances in cryptology for e-cash, since 2007; with France Télécom R&D, Gemalto, NXP Semiconductors, Cryptolog International, École normale supérieure Paris and Université Caen

8. Other Grants and Activities

8.1. Network of excellence

Together with the SECRET project at INRIA Rocquencourt, the project TANC has taken part in ECRYPT, a NoE in the Information Society Technologies theme of the 6th European Framework Programme (FP6).

8.2. ANR

CADO (since 2006-09-01): two meetings (18-19/01/07 in Nancy for the kickoff and 21-21/06/07 in Paris).

8.3. Associated team

The TANC project is involved in the associated team ECHECS ("Extreme Computing for (Hyper-)Elliptic Cryptographic Systems") with É. Schost of University of Western Ontario, London, continuing a long-standing collaboration. Our joint work is concerned with using advanced algorithms of symbolic computation (speciality of the Canadian team) in the context of elliptic and hyperelliptic curve cryptography (speciality of TANC), in particular for the instantiation of secure cryptosystems.

As part of this collaboration, L. De Feo visited twice University of Western Ontario (march 2008, november-december 2008) to work with E. Schost on fast symbolic algorithms for isogeny computation.

8.4. OMT

TANC, together with the Hipercom EPI, has started an OMT (offre de maturation technologique) financed by Digiteo. The aim of the Cryptonet OMT is to realize a proof of concept of the use of elliptic curves over finite fields in providing security on ad hoc networks. The main interest of elliptic curves in that setting is the low cost and (a priori) low bandwith required for a given level of security, as compared to traditional finite field based systems. The engineer attached to this project will inject our knowledge into a standard network simulator. Scientific details are provided in Section 6.4.

The project brings very short signature to OLSR, and such a small size may have non negative impact on the network performance. Testing of such small signatures is in progress.

The code is in java and is integrated in the Java OLSRv2 implementation of Hipercom. We use the java framework for cryptography, which enables us to use any signature algorithm, not necessarly ours.

9. Dissemination

9.1. Programme committees

A. Enge took part in the programme committee of Pairing 2008 – International Conference on Pairing-Based Cryptography at Royal Holloway University of London. He acted on the scientific advisary board of the Journées Nationales de Calcul Formel 2008 at Luminy.

9.2. Teaching

François Morain was in charge of half of the 2nd year course "Algorithmes et Programmation: du séquentiel au distribué", together with J.-M. Steyaert. He gives a cryptology course in Majeure 2. He is vice-head of the Département d'Informatique. He has been representing École polytechnique in the Commission des Études du Master MPRI, since its creation in 2004.

At École polytechnique, A. Enge has proposed computer science labs for the second year course "Algorithmes et Programmation: du séquentiel au distribué". He has developed the practical module for the master level cryptology course, centred around securing a network application in the Java cryptography framework JCE.

B. Smith taught the module on elliptic curve cryptography and pairings in the MPRI course on Cryptologie.

Daniel Augot taught an introductory course of cryptography (Master 2) at Université de Marne la vallée. He also gave some lectures on algebraic coding theory in the MPRI Master 2. He also gave a lecture in the context of a cycles of lectures on cryptology for tunisian officers, organized by Thales.

9.3. Seminars and talks

Daniel Augot gave a talk "Algorithme de Guruswami-Sudan et généralisations multivariées" au séminaire de de l'IRMAR (Université de Rennes). He was invited at the University of Zürich (Joachim Rosenthal), and gave a talk on key equations for the Guruswami-Sudan list decoding algorithm.

[17] has been presented at ANTS-VIII in Banff by A. Enge; it has been rewarded by the Selfridge Prize of the Number Theory Foundation for the best paper.

A. Enge has given an invited lecture on "Discrete logarithms in curves: from $L(1/2)$ to $L(1/3)$" at the Third Franco-Japanese Computer Security Workshop at Nancy.

He has given three lectures entitled "Un algorithme en $L(1/3+\varepsilon)$ pour le problème du logarithme discret dans certaines courbes" at the seminar Arithmétique et théorie de l'information at Luminy, the cryptography seminar at Rennes and the seminar Arith at Montpellier.

A. Enge has spoken on "Constructions de courbes algébriques pour la cryptographie" at the number theory seminar of Marrakech.

F. Morain spent a week in Tokyo (Chuo University) and gave a talk on *Recent improvements to the SEA algorithm in genus 1*. F. Morain was invited speaker for ANTS8 in Banff (May 2008); his talk was *survey on algorithms for computing isogenies on low genus curves*.

L. De Feo gave a lecture on "Fast arithmetics in Artin-Schreier towers over finite fields" at C4 in École Polytechnique. He gave a lecture on "Transposition principle" at Journées nationales de calcul formel 2008 held in Luminy.

J.F. Biasse also gave a lecture on "Logarithme discret dans les courbes hyperelliptiques" at Journées nationales de calcul formel 2008 held in Luminy.

B. Smith presented the research in [18] at EUROCRYPT 2008 in Istanbul, where it won the best paper award. He gave an invited talk on discrete logarithms on genus 3 curves in the special session on low-genus curves and applications of the 2008 Joint Meetings of the American Mathematical Society and the Mathematical Association of America in San Diego, and also gave a talk on the same subject in the Séminaire de Cryptologie at the Université de Caen.

9.4. Vulgarisation and Summer schools

B. Smith gave two lectures on advanced topics in elliptic curves at the DIAMANT Summer School on Elliptic and Hyperelliptic Curve Cryptography in September 2008 in Eindhoven.

B. Smith has given a lecture on pairings on elliptic curves at the 3rd ECRYPT PhD Summer School on Advanced Topics in Cryptography in May 2008 on Crete.

A. Enge has taken part in the school “Référentiels de la cryptographie moderne” organised from October 28 to 31 in Rabat by the Association Marocaine de Cryptographie with a lecture series on pairings entitled “Couplages sur les courbes elliptiques — Fondements mathématiques et calcul”.

9.5. Editorship

A. Enge is editor of “Designs, Codes and Cryptography” since 2004.

Daniel Augot is guest editor, with Jean-Charles Faugère and Ludovic Perret of a special issue of the Journal of Symbolic Computation, on Gröbner Bases Techniques in Cryptography and Coding Theory.

9.6. Awards

B. Smith has received the best paper award for [18] at Eurocrypt 2008 in Istanbul. He has been invited to submit an extended version [14] to the Journal of Cryptology.

A. Enge has received the Selfridge Prize of the Number Theory Foundation for the best paper [17] presented at Algorithmic Number Theory Symposium — ANTS-VIII in Banff.

9.7. Thesis committees

F. Morain was the president of the defense committee for F. Didier (19/12/2007).

9.8. Research administration

A. Enge is correspondent for European affairs of INRIA Saclay–Île-de-France (formerly INRIA Futurs) since 2006 and correspondent for international affairs since 2007.

F. Morain represents INRIA in the “Conseil d’UFR 929 Maths Université Paris 6” since September 2005.

10. Bibliography

Major publications by the team in recent years

[1] A. BASIRI, A. ENGE, J.-C. FAUGÈRE, N. GÜREL. *The Arithmetic of Jacobian Groups of Superelliptic Cubics*, in "Math. Comp.", vol. 74, 2005, p. 389–410, https://hal.inria.fr/inria-00071967.

[2] A. ENGE, P. GAUDRY. *A general framework for subexponential discrete logarithm algorithms*, in "Acta Arith.", vol. CII, n^{o} 1, 2002, p. 83–103.

[3] A. ENGE, P. GAUDRY. *An $L(1/3+\varepsilon)$ algorithm for the discrete logarithm problem for low degree curves*, in "Advances in Cryptology — Eurocrypt 2007, Berlin", M. NAOR (editor), Lecture Notes in Comput. Sci., vol. 4515, Springer-Verlag, 2007, p. 379–393, http://hal.inria.fr/inria-00135324.

[4] A. ENGE, F. MORAIN. *Comparing Invariants for Class Fields of Imaginary Quadratic Fields*, in "Algorithmic Number Theory", C. FIEKER, D. R. KOHEL (editors), Lecture Notes in Comput. Sci., 5th International Symposium, ANTS-V, Sydney, Australia, July 2002, Proceedings, vol. 2369, Springer-Verlag, 2002, p. 252–266.

[5] A. ENGE, R. SCHERTZ. *Constructing elliptic curves over finite fields using double eta-quotients*, in "Journal de Théorie des Nombres de Bordeaux", vol. 16, 2004, p. 555–568, http://www.lix.polytechnique.fr/Labo/Andreas.Enge/vorabdrucke/cm.ps.gz.

[6] P. MIHĂILESCU, F. MORAIN, É. SCHOST. *Computing the eigenvalue in the Schoof-Elkies-Atkin algorithm using Abelian lifts*, in "ISSAC '07: Proceedings of the 2007 international symposium on Symbolic and algebraic computation, New York, NY, USA", ACM Press, 2007, p. 285–292, http://hal.inria.fr/inria-00130142.

[7] F. MORAIN. *La primalité en temps polynomial [d'après Adleman, Huang; Agrawal, Kayal, Saxena]*, in "Astérisque", Séminaire Bourbaki. Vol. 2002/2003, n^{o} 294, 2004, p. Exp. No. 917, 205–230.

[8] F. MORAIN. *Computing the cardinality of CM elliptic curves using torsion points*, in "Journal de Théorie des Nombres de Bordeaux", vol. 19, n^{o} 3, 2007, p. 663–681, http://arxiv.org/ps/math.NT/0210173.

[9] F. MORAIN. *Implementing the asymptotically fast version of the elliptic curve primality proving algorithm*, in "Math. Comp.", vol. 76, 2007, p. 493–505.

Year Publications

Articles in International Peer-Reviewed Journal

[10] A. BOSTAN, F. MORAIN, B. SALVY, É. SCHOST. *Fast algorithms for computing isogenies between elliptic curves*, in "Math. Comp.", vol. 77, 2008, p. 1755–1778.

[11] R. DUPONT. *Fast evaluation of modular functions using Newton iterations and the AGM*, in "Math. Comp.", To appear, 2008, http://www.lix.polytechnique.fr/Labo/Regis.Dupont/preprints/Dupont_FastEvalMod.ps.gz.

[12] A. ENGE. *Computing modular polynomials in quasi-linear time*, in "Mathematics of Computation", To appear, 2008.

[13] A. ENGE. *The complexity of class polynomial computation via floating point approximations*, in "Mathematics of Computation", To appear, 2008.

[14] B. SMITH. *Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves*, in "J. of Cryptology", To appear, 2008.

Invited Conferences

[15] A. ENGE. *Discrete logarithms in curves over finite fields*, in "Finite Fields and Applications", G. L. MULLEN, D. PANARIO, I. E. SHPARLINSKI (editors), Contemporary Mathematics, vol. 461, American Mathematical Society, 2008, p. 119–139.

International Peer-Reviewed Conference/Proceedings

[16] D. AUGOT, A. ZEH. *On the Roth and Ruckenstein equations for the Guruswami-Sudan algorithm*, in "Information Theory, 2008. ISIT 2008. IEEE International Symposium on", 2008, p. 2620–2624, http://dx.doi.org/10.1109/ISIT.2008.4595466.

[17] J. BELDING, R. BRÖKER, A. ENGE, K. LAUTER. *Computing Hilbert class polynomials*, in "Algorithmic Number Theory - ANTS-VIII, Berlin", A. VAN DER POORTEN, A. STEIN (editors), Lecture Notes in Computer Science, vol. 5011, Springer-Verlag, 2008, p. 282–295.

[18] B. SMITH. *Isogenies and the Discrete Logarithm Problem in Jacobians of Genus 3 Hyperelliptic Curves*, in "Advances in Cryptology - EUROCRYPT 2008", N. SMART (editor), Lecture Notes in Comput. Sci., vol. 4965, Springer, 2008, p. 163-180.

Other Publications

[19] THE CADO TEAM. *CADO — Number field sieve: distribution, optimization*, 2008, http://cado.gforge.inria.fr/.

References in notes

[20] *Digital Signature Standard (DSS)*, Technical report, n^{o} FIPS PUB 186-3, National Institute of Standards and Technology, 2006.

[21] L. M. ADLEMAN, J. DEMARRAIS, M.-D. HUANG. *A Subexponential Algorithm for Discrete Logarithms over the Rational Subgroup of the Jacobians of Large Genus Hyperelliptic Curves over Finite Fields*, in "Algorithmic Number Theory, Berlin", L. M. ADLEMAN, M.-D. HUANG (editors), Lecture Notes in Comput. Sci., vol. 877, Springer-Verlag, 1994, p. 28–40.

[22] P. S. L. M. BARRETO, B. LYNN, M. SCOTT. *Constructing Elliptic Curves with Prescribed Embedding Degrees*, in "Security in Communication Networks — Third International Conference, SCN 2002, Amalfi, Italy, September 2002, Berlin", S. CIMATO, C. GALDI, G. PERSIANO (editors), Lecture Notes in Comput. Sci., vol. 2576, Springer-Verlag, 2003, p. 257–267.

[23] D. BERNSTEIN. *Proving primality in essentially quartic expected time*, in "Math. Comp.", vol. 76, 2007, p. 389–403.

[24] D. BONEH, B. LYNN, H. SHACHAM. *Short signatures from the Weil pairing*, in "Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings", C. BOYD (editor), Lecture Notes in Computer Science, vol. 2248, Springer, 2001, p. 514-532.

[25] A. BOSTAN, P. GAUDRY, É. SCHOST. *Linear recurrences with polynomial coefficients and computation of the Cartier-Manin operator on hyperelliptic curves*, in "Finite Fields and Applications, 7th International Conference, Fq7", G. MULLEN, A. POLI, H. STICHTENOTH (editors), Lecture Notes in Comput. Sci., vol. 2948, Springer-Verlag, 2004, p. 40–58, http://www.lix.polytechnique.fr/Labo/Pierrick.Gaudry/publis/cartierFq7.ps.gz.

[26] C. CLAUSEN, P. JACQUET. *The Optimized Link State Routing Protocol version 2*, Technical report, IETF Draft, 2008.

[27] S. CONTINI. *Factoring integers with the self-initializing quadratic sieve*, 1997, http://citeseer.ist.psu.edu/contini97factoring.html.

[28] J.-M. COUVEIGNES. *Algebraic Groups and Discrete Logarithm*, in "Public-Key Cryptography and Computational Number Theory, Berlin", K. ALSTER, J. URBANOWICZ, H. C. WILLIAMS (editors), De Gruyter, 2001, p. 17–27.

[29] J.-M. COUVEIGNES. *Quelques calculs en théorie des nombres*, Thèse, Université de Bordeaux I, July 1994.

[30] J.-M. COUVEIGNES. *Computing l-isogenies using the p-torsion*, in "Algorithmic Number Theory", H. COHEN (editor), Lecture Notes in Comput. Sci., Second International Symposium, ANTS-II, Talence, France, May 1996, Proceedings, vol. 1122, Springer Verlag, 1996, p. 59–65.

[31] C. DIEM. *An Index Calculus Algorithm for Plane Curves of Small Degree*, in "Algorithmic Number Theory — ANTS-VII, Berlin", F. HESS, S. PAULI, M. POHST (editors), Lecture Notes in Computer Science, vol. 4076, Springer-Verlag, 2006, p. 543–557.

[32] R. DUPONT. *Moyenne arithmético-géométrique, suites de Borchardt et applications*, Ph. D. Thesis, École polytechnique, 2006.

[33] R. DUPONT, A. ENGE, F. MORAIN. *Building curves with arbitrary small MOV degree over finite prime fields*, in "J. of Cryptology", vol. 18, n^{o} 2, 2005, p. 79–89, http://www.lix.polytechnique.fr/Labo/Andreas.Enge/vorabdrucke/mov.ps.gz.

[34] A. ENGE. *A General Framework for Subexponential Discrete Logarithm Algorithms in Groups of Unknown Order*, in "Finite Geometries, Dordrecht", A. BLOKHUIS, J. W. P. HIRSCHFELD, D. JUNGNICKEL, J. A. THAS (editors), Developments in Mathematics, vol. 3, Kluwer Academic Publishers, 2001, p. 133–146.

[35] A. ENGE. *Computing Discrete Logarithms in High-Genus Hyperelliptic Jacobians in Provably Subexponential Time*, in "Math. Comp.", vol. 71, n^{o} 238, 2002, p. 729–742.

[36] A. ENGE, F. MORAIN. *Fast decomposition of polynomials with known Galois group*, in "Applied Algebra, Algebraic Algorithms and Error-Correcting Codes", M. FOSSORIER, T. HØHOLDT, A. POLI (editors), Lecture Notes in Comput. Sci., 15th International Symposium, AAECC-15, Toulouse, France, May 2003, Proceedings, vol. 2643, Springer-Verlag, 2003, p. 254–264.

[37] C. FONTAINE, F. GALAND. *How Can Reed-Solomon Codes Improve Steganographic Schemes?*, in "Information Hiding", T. FURON, F. CAYRE, G. DOËRR, P. BAS (editors), Lecture Notes in Computer Science, n^{o} 4567, Springer Berlin / Heidelberg, 2007, p. 130–144, http://www-rocq.inria.fr/secret/Frederic.Didier/machines.php.

[38] J. FRANKE, T. KLEINJUNG, F. MORAIN, T. WIRTH. *Proving the primality of very large numbers with fastECPP*, in "Algorithmic Number Theory", D. BUELL (editor), Lecture Notes in Comput. Sci., 6th International Symposium, ANTS-VI, Burlington, VT, USA, June 2004, Proceedings, vol. 3076, Springer-Verlag, 2004, p. 194–207.

[39] P. GAUDRY, N. GÜREL. *Counting points in medium characteristic using Kedlaya's algorithm*, in "Experiment. Math.", vol. 12, n^{o} 4, 2003, p. 395–402, http://www.expmath.org/expmath/volumes/12/12.html.

[40] P. GAUDRY. *An Algorithm for Solving the Discrete Log Problem on Hyperelliptic Curves*, in "Advances in Cryptology — EUROCRYPT 2000, Berlin", B. PRENEEL (editor), Lecture Notes in Comput. Sci., vol. 1807, Springer-Verlag, 2000, p. 19–34.

[41] P. GAUDRY. *A comparison and a combination of SST and AGM algorithms for counting points of elliptic curves in characteristic 2*, in "Advances in Cryptology – ASIACRYPT 2002", Y. ZHENG (editor), Lecture Notes in Comput. Sci., vol. 2501, Springer–Verlag, 2002, p. 311–327.

[42] P. GAUDRY, F. MORAIN. *Fast algorithms for computing the eigenvalue in the Schoof-Elkies-Atkin algorithm*, in "ISSAC '06: Proceedings of the 2006 international symposium on Symbolic and algebraic computation, New York, NY, USA", ACM Press, 2006, p. 109–115, http://hal.inria.fr/inria-00001009.

[43] P. GAUDRY, É. SCHOST. *Construction of Secure Random Curves of Genus 2 over Prime Fields*, in "Advances in Cryptology – EUROCRYPT 2004", C. CACHIN, J. CAMENISCH (editors), Lecture Notes in Comput. Sci., vol. 3027, Springer-Verlag, 2004, p. 239–256, http://www.lix.polytechnique.fr/Labo/Pierrick.Gaudry/publis/secureg2.ps.gz.

[44] P. GAUDRY, É. SCHOST. *Modular equations for hyperelliptic curves*, in "Math. Comp.", vol. 74, 2005, p. 429–454, http://www.lix.polytechnique.fr/Labo/Pierrick.Gaudry/publis/eqmod2.ps.gz.

[45] P. GAUDRY, E. THOMÉ, N. THÉRIAULT, C. DIEM. *A double large prime variation for small genus hyperelliptic index calculus*, in "Math. Comp.", vol. 76, 2007, p. 475–492, http://www.loria.fr/~gaudry/publis/dbleLP.ps.gz.

[46] J. E. GOWER, S. S. WAGSTAFF, JR.. *Square form factorization*, in "Math. Comp.", vol. 77, 2008, p. 551–588.

[47] V. GURUSWAMI, M. SUDAN. *Improved decoding of Reed-Solomon and algebraic-geometry codes*, in "IEEE Transactions on Information Theory", vol. 45, n^{o} 6, 1999, p. 1757–1767.

[48] U. HERBERG. *JOLSRv2: An OLSRv2 implementation in Java*, in "4th OLSR Interop Workshop, Ottawa, Canada", 2008.

[49] F. HESS. *Computing Relations in Divisor Class Groups of Algebraic Curves over Finite Fields*, Draft version, 2004, http://www.math.tu-berlin.de/~hess/personal/dlog.ps.gz.

[50] T. HØHOLDT, J. H. VAN LINT, R. PELLIKAAN. *Algebraic geometry codes*, in "Handbook of Coding Theory", vol. I, Elsevier, 1998, p. 871–961.

[51] D. JAO, S. D. MILLER, R. VENKATESAN. *Do All Elliptic Curves of the Same Order Have the Same Difficulty of Discrete Log?*, in "ASIACRYPT", Lecture Notes in Comput. Sci., 2005, p. 21-40.

[52] A. JOUX. *A One Round Protocol for Tripartite Diffie–Hellman*, in "Algorithmic Number Theory — ANTS-IV, Berlin", W. BOSMA (editor), Lecture Notes in Comput. Sci., vol. 1838, Springer-Verlag, 2000, p. 385–393.

[53] H. W. JR. LENSTRA, C. POMERANCE. *Primality testing with Gaussian periods*, Preliminary version, July 2005, http://www.math.dartmouth.edu/~carlp/PDF/complexity072805.pdf.

[54] R. LERCIER. *Computing isogenies in F_{2^n}*, in "Algorithmic Number Theory", H. COHEN (editor), Lecture Notes in Comput. Sci., Second International Symposium, ANTS-II, Talence, France, May 1996, Proceedings, vol. 1122, Springer Verlag, 1996, p. 197–212.

[55] R. LERCIER, F. MORAIN. *Computing isogenies between elliptic curves over F_{p^n} using Couveignes's algorithm*, in "Math. Comp.", vol. 69, n^{o} 229, January 2000, p. 351–370.

[56] J. MCKEE. *Speeding Fermat's Factoring Method*, in "Math. Comp.", vol. 68, n^{o} 228, October 1999, p. 1729-1737.

[57] F. MORAIN. *Elliptic curves for primality proving*, in "Encyclopedia of cryptography and security", H. C. A. VAN TILBORG (editor), Springer, 2005.

[58] M. A. MORRISON, J. BRILLHART. *A method of factoring and the factorization of F_7*, in "Math. Comp.", vol. 29, n^{o} 129, January 1975, p. 183-205.

[59] A. ROSTOVTSEV, A. STOLBUNOV. *Public-key cryptosystem based on isogenies*, 2006, http://eprint.iacr.org/, Cryptology ePrint Archive, Report 2006/145.

[60] R. SAKAI, K. OHGISHI, M. KASAHARA. *Cryptosystems based on pairing*, SCIS 2000, The 2000 Symposium on Cryptography and Information Security, Okinawa, Japan, January 26–28, 2000.

[61] A. SUTHERLAND. *Computing Hilbert class polynomials with the CRT method*, Talk at the 12th Workshop on Elliptic Curve Cryptography (ECC), 2008, http://www.hyperelliptic.org/tanja/conf/ECC08/slides/Andrew-V-Sutherland.pdf.

[62] E. TESKE. *An elliptic trapdoor system*, in "J. of Cryptology", vol. 19, n^{o} 1, 2006, p. 115–133.

[63] Y. WU. *New List Decoding Algorithms for Reed-Solomon and BCH Codes*, in "Information Theory, IEEE Transactions on", vol. 54, n^{o} 8, 2008, p. 3611–3630, http://dx.doi.org/10.1109/TIT.2008.926355.