INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

# *Project-Team TANC*

# *Théorie Algorithmique des Nombres pour la Cryptologie*

*Futurs*

THEME SYM

# Table of contents

# 1. Team

**Team Leader**
François Morain [ Professor at École polytechnique, HdR ]

**Staff member INRIA**
Andreas Enge [ CR1, HdR ]

**Doctoral students**
Thomas Houtmann [ CNRS/DGA since 2004-10-01 ]
Luca De Feo [ École polytechnique since 2007-09-01 ]
Jean-François Biasse [ DGA since 2007-09-01 ]

**Administrative Assistant**
Évelyne Rayssac [ École polytechnique ]

**External researchers**
Daniel Augot [ CR1, Projet CODES ]

**Junior technical staff**
Jérôme Milan [ Ingénieur associé since 2005-10-01 ]

**Student intern**
Luca De Feo [ stagiaire MPRI, April–August 2007 ]
Jean-François Biasse [ stagiaire MPRI, April–August 2007 ]
Guillaume Guerpillon [ École polytechnique, April –July 2007 ]

**Visitors**
Ben Smith [ Royal Holloway, from 2007-02-05/09 ]
Igor Shparlinski [ Macquarie University, 2007-09-07/14 ]

# 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 sentence 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 points 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 or hyperelliptic cryptosystems.
- Pairings: The new number theoretic primitive of pairings (i.e., bilinear functions) on algebraic curves enables plenty of novel applications and poses algorithmic challenges concerning efficient implementations and the creation of secure instances.

## 2.2. Exploratory topics

As described in the name of our project, we aim at providing robust primitives for asymmetric cryptography. In recent years, we have made several attempts at coming closer to another part of cryptology, by applying our knowledge to real life protocols. We are currently trying to promote the use of elliptic curves in environments where this could be useful, namely *ad hoc* networks.

In another direction, Daniel Augot is studying the decoding of error correcting codes based on algebraic curves (algebraic geometry codes). These codes are a successful generalization of the Reed-Solomon codes, because they provide good error correction capacities. The main drawback of these codes is that the known decoding algorithms of these codes have a too large complexity, that is to say, higher than quadratic in terms of the length of the code. Project-Team TANC has successfully used techniques and advanced algorithms from computer algebra to obtain fast algorithms in the domain of cryptography. Daniel Augot plans to build upon this knowledge to get efficient decoding algorithms of algebraic geometry codes. The first step is to efficiently decode Hermitian codes, whose decoding complexity is currently in $O(n^{7/3})$. These codes are indeed the most understood of AG codes, and they are also good candidates for using the Guruswami-Sudan principles for list-decoding.

## 2.3. Highlights of the year

For the very first time in algebraic curve cryptography, A. Enge and P. Gaudry (CACAO) have exhibited a class of curves in which the discrete logarithm problem is attacked by a subexponential algorithm of complexity ressembling that of the most powerful algorithms that break the famous RSA cryptosystem. This makes the corresponding algebraic curve cryptosystems no more secure than RSA. This result is a major step towards the goal of the TANC project to catalogue all classes of curves suited for cryptography. The publication [12] was rewarded as one of the three best papers at the Eurocrypt 2007 conference.

# 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. Old 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: computing $E$ and $D$ must be doable 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 arithmetical problems. There we find the integer factoring problem, the discrete logarithm problem, etc. 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. Part of what follows does not depend on this setting, and can be used as is over the rationals, for instance.

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 what is called the *tangent-and-chord* formulae. 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.

A. Enge and N. Gürel have worked with J. -C. Faugère and A. Basiri (LIP 6) on the arithmetic of superelliptic and $C_{a,b}$ curves, the next complex class of algebraic curves after the well understood hyperelliptic ones. They have dramatically improved the existing algorithms and have found new algorithms for superelliptic cubic curves, that is, curves of the form $y^3 = f(x)$ with $\deg(f)$ prime to 3 and at least 4 [1]. They have generalized their work, in part based on Gröbner basis computations, to $C_{3,4}$ curves and have provided explicit formulae for realizing the group law using only operations in the underlying (finite) field [22].

The great catalog of usable curves is 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 [44].

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 [8]. To get one step further, one needs to use genus 2 analogues of modular equations. After a theoretical study [9], 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 [24]. 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 [48]. Recently, there appeared suggestions to use isogenies in a cryptographic context, replacing the multiplication on curves by the use of such morphisms [58], [56].

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 [27], [28], [52] and one to Lercier [51].

### *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 [19], and A. Enge has developed the first algorithm with a proven subexponential run time of $L(1/2)$ in [33]. 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 [35], [32]. Proofs for arbitrary curves of large genus are given by J.-M. Couveignes [26] and F. Heß (see [47]).

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.

### *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 [49] and identity based encryption [57]. 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 [31], the other one being developed in [21].

## 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 [31].

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 [36]). 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 [37]. These invariants, together with this new algorithm, are incorporated in the working version of the program ECPP.

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 [29].

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.

# 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 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.lix.polytechnique.fr/Labo/Andreas.Enge/Software.html

The latest version 0.4.6 has been released in September 2007. The library currently benefits from an Opération de développement logiciel of INRIA.

The `mpc` library is used in our team to build curves with complex multiplication and to compute modular polynomials (cf. Section 6.1.1), and it is *de facto* incorporated in the ECPP program.

## 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,

and 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 [18] 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 [55]) |
| Fermat | (McKee's "fast" variant of Fermat's algorithm [53]) |
| QS | (Quadratic Sieve [25]) |
| SIQS | (Self-Initializing Quadratic Sieve [25]) |
| 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. However, it should be

stressed that our implementation of SIQS still lags behind performance-wise with respect to the competition. We stand committed to address this shortcoming in the near term.

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.

The new record of SEA is currently (September 2007) for a prime $p$ of 2500 decimal digits (again compared to 500dd back in 1995), using the work in [15] (see below), as well as [13], in which a new approach to the eigenvalue computation is described and proven.

A crucial ingredient for these records was A. Enge's new algorithm [14] 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 [15]. 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 medium characteristic.

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, has been cleaning the most recent of them, known as CouveignesII, that 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, and a fresh implementation in NTL is needed, that will be his first thesis work. A publication on the first results obtained is in preparation.

### *6.1.3. Discrete logarithms on curves*

**Participant:** Andreas Enge.

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 $L(1/2)$. 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 result is a major step towards the goal of the TANC project to catalogue all classes of curves suited for cryptography. The publication [12] was rewarded as one of the three best papers at the Eurocrypt 2007 conference, and we are invited to submit an extended version to *Journal of Cryptology*. A comparative implementation of the different algorithms of complexity $L(1/2)$ resp. $L(1/3)$ is underway by a master student of A. Enge's, J.-F. Biasse.

## 6.2. Complex multiplication

### 6.2.1. Genus 1

**Participants:** Andreas Enge, François Morain.

The work of AKS motivated the work of F. Morain on a fast variant of ECPP, called fastECPP, which led him to gain one order of magnitude in the complexity of the problem (see [11] [54]), 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 [50] 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 [11], 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.

A. Enge has been able to analyze precisely the complexity of class polynomial computations via complex floating point approximations. In fact, this approach has recently been challenged by algorithms using $p$-adic liftings, that achieve a running time that is (up to logarithmic factors) linear in the output size. He has shown that the algorithm using complex numbers, in its currently implemented form, has a slightly worse asymptotic complexity (polynomial with exponent $1.25$). Using techniques from fast symbolic computation, namely multievaluation of polynomials, he has obtained an asymptotically optimal (up to logarithmic factors) algorithm with floating point approximations. The implementation has shown, however, that in the currently practical range, the asymptotically fast algorithm is slower than the previous one. This is due, on the one hand, to the multitude of algorithmic improvements introduced in [36], and on the other hand, to the lack of logarithmic factors and better constants.

Using R. Dupont's results [30], A. Enge has devised a second quasi-linear algorithm (that actually even saves a logarithmic factor in the complexity). Breaking the record for class polynomial computations, he has computed a polynomial of degree 100,000, the largest coefficient of which has almost 250,000 bits. For this enormous example, the asymptotically fast algorithm finally beats the one with exponent 1.25. The implementation is based on GMP, mpfr and mpc (see Section 5.2) and a library of A. Enge's for fast arithmetic with polynomials over multiprecision floating point numbers. It turns out that the algorithms are so optimized that the limiting factor becomes the memory consumption [34].

### 6.2.2. Genus 2

**Participant:** Thomas Houtmann.

P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler and A. Weng [42], [43] have designed a new approach to construct class polynomials of genus two curves having complex multiplication. The main feature of their method is the use of 2-adic numbers instead of complex floating-point approximations. Although that method suffers from limitations due to the fact that its initialisation highly depends of the splitting of 2 in the quartic CM field, the corresponding algorithm is very efficient compared to previous approaches.

T. Houtmann worked on both the aspects for an alternative to $p$-adic method and classical CM method. He improved the period matrices computation phase, collaborated with R. Dupont to improve the analytic phase and did work on using the very method to generate hyperelliptic curves suitable for cryptography. As far as his work is advanced, he managed to compute a 132-degree Igusa class polynomial system.

## 6.3. Identity cards of elliptic curves

One of the main goals of the TANC project is to determine the *identity card* of an elliptic curve, that collects and certifies properties of potential relevance for its cryptographic security. These include the cardinality (see Section 6.1.1) and the endomorphism ring (cf. Section 6.2 on complex multiplication, that permits to construct a curve with a given endomorphism ring).

For a random curve, the class group of its endomorphism ring, an order in an imaginary quadratic number field, is of interest; some cryptographic standards, for instance, prescribe a minimum size of this class group [20]. G. Guerpillon, master student of A. Enge's, has implemented and optimised a subexponential algorithm for computing these class groups. The currently undertaken parallelisation of his implementation should enable us to reach a new record for this kind of computation. One of the main ingredients, the Hermite normal form computation of an integral matrix, has been reused by J.-F. Biasse in the context of discrete logarithms on $C_{a,b}$ curves, see Section 6.1.3.

The subexponential algorithm returns the group as a product of cyclic groups with their generators. For the case when all elements need to be explicitly enumerated, A. Enge has developed quasi-linear algorithms in [34].

## 6.4. Security in ad hoc networks

**Participants:** François Morain, Daniel Augot.

F. Morain and D. Augot (CODES) participate in the ACI SERAC (SEcuRity models and protocols for Ad-hoC Networks), which started in september 2004. Their interest there is to understand the (new?) cryptographic needs required and to try to invent new trust models.

It is clear that the recent arrival of HIPERCOM (also a member of SERAC) at École polytechnique triggers new collaborations in that direction.

Achieving secure routing in ad-hoc networks is a big challenge. The typical way to prevent or reduce the possible attacks is to use mechanisms to authenticate the origin of all messages. Standard (asymmetric) signature schemes provide these mechanisms, but may result in inefficient implementations, especially when many nodes (and so many signatures) are expected.

# 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.

# 8. Other Grants and Activities

## 8.1. Network of excellence

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

J. Herranz and F. Laguillaumie have participated in the AZTEC working group WG3 on asymmetric techniques with special properties on November 23–24.

F. Laguillaumie participated in the WG3 of NEO ECRYPT (July 16-17).

## 8.2. ACI

- ACI SÉCURITÉ SERAC: SEcuRity models and protocols for Ad-hoC networks (since 2004-09-01).

## 8.3. ANR

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

## 8.4. 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.

## 8.5. 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.

# 9. Dissemination

## 9.1. Program committees

A. Enge took part in the program committees of Pairing 2007 – First International Conference on Pairing-Based Cryptography in Tokio and WCC 2007 – International Workshop on Coding and Cryptography in Versailles. He acted on the scientific advisary board of the Journées Nationales de Calcul Formel 2007 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 first year course "Introduction à l'informatique". He has developed the practical module for the master level cryptology course, centred around securing a network application in the Java cryptography framework JCE.

## 9.3. Seminars and talks

F. Morain has been invited as a plenary lecturer to the "Workshop on Computational challenges arising in algorithmic number theory and Cryptography", October 30- November 3, 2006, in the Fields Institute in Toronto (Canada). There he presented [13].

A. Enge has been invited as a plenary lecturer to ACISP 2007 – 12th Australasian Conference on Information Security and Privacy at Townsville, Australia, with a talk entitled "Constructing cryptographic curves"; and to Fq8 – 8th International Conference on Finite Fields and Applications at Melbourne, speaking on "The discrete logarithm problem for algebraic curves".

[12] has been presented at Eurocrypt 2007 in Barcelona by A. Enge; it has been elected as one of the three best papers of the conference by the program committee. A. Enge has given two lectures on “Constructing elliptic curves by complex multiplication” and “Subexponential discrete logarithm algorithms for finite fields” at the ICE-EM RNSA Workshop on Pairing Based Cryptography, Brisbane, Australia.

## 9.4. Editorship

A. Enge is editor of “Designs, Codes and Cryptography”. He has co-edited the special issue “Algorithmic Number Theory and Its Applications” of the Japan Journal of Industrial and Applied Mathematics.

## 9.5. Thesis committees

F. Morain was in the thesis committee of Bassem Sakkour (2007-04-06) and of Cédric Lauradoux (2007-06-22); in the HdR committee for P. Loidreau (2007-01-25); D. Augot (2007-06-07).

## 9.6. Research administration

A. Enge is a member of the International Relations Working Group (GTRI) at the Scientific and Technological Orientation Council (COST) of INRIA. As such, he regularly participates in the selection of postdoc positions for the European ERCIM consortium and of international Associated teams. He also acts as the scientific representative for European affairs at INRIA Saclay.

F. Morain represents INRIA in the “Conseil d’UFR 929 Maths Université Paris 6” since September 2005. F. Morain participated in the evaluation of the *Unité de Mathématiques Appliquées* of ENSTA (05/07/06).

# 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. *Elliptic Curves and Their Applications to Cryptography — An Introduction*, Kluwer Academic Publishers, 1999.

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

[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. GAUDRY, N. GÜREL. *An extension of Kedlaya's point counting algorithm to superelliptic curves*, in "Advances in Cryptology – ASIACRYPT 2001", C. BOYD (editor), Lecture Notes in Comput. Sci., vol. 2248, Springer-Verlag, 2001, p. 480–494.

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

[8] 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.

[9] 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.

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

# Year Publications

## Articles in refereed journals and book chapters

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

## Publications in Conferences and Workshops

[12] 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 Computer Science, vol. 4515, Springer-Verlag, 2007, p. 367–382, http://hal.inria.fr/inria-00135324.

[13] 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.

## Internal Reports

[14] A. ENGE. *Computing modular polynomials in quasi-linear time*, HAL-INRIA, n° 143084 et ArXiv 0704.3177, INRIA, 2007, http://hal.inria.fr/inria-00143084.

## Miscellaneous

[15] A. BOSTAN, F. MORAIN, B. SALVY, É. SCHOST. *Fast algorithms for computing isogenies between elliptic curves*, To appear in Math. Comp., June 2007, https://hal.inria.fr/inria-00091441.

[16] R. DUPONT. *Fast evaluation of modular functions using Newton iterations and the AGM*, To appear in Math. Comp., 2007, http://www.lix.polytechnique.fr/Labo/Regis.Dupont/preprints/Dupont_FastEvalMod.ps.gz.

[17] F. MORAIN. *Computing the cardinality of CM elliptic curves using torsion points*, To appear in J. Théor. Nombres Bordeaux., June 2007, http://arxiv.org/ps/math.NT/0210173.

[18] THE CADO TEAM. *ANR CADO*, 2007.

## References in notes

[19] 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.

[20] BSI (BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK). *Geeignete Kryptoalgorithmen gemäß § 17 (2) SigV*, 1999.

[21] 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.

[22] A. BASIRI, A. ENGE, J.-C. FAUGÈRE, N. GÜREL. *Implementing the Arithmetic of $C_{3,4}$ Curves*, in "Algorithmic Number Theory — ANTS-VI, Berlin", D. BUELL (editor), Lecture Notes in Comput. Sci., vol. 3076, Springer-Verlag, 2004, p. 87–101, http://www.lix.polytechnique.fr/Labo/Andreas.Enge/C34.html.

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

[24] 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.

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

[26] 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.

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

[28] 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.

[29] R. DUPONT. *Fast evaluation of modular functions using Newton iterations and the AGM*, To appear in Math. Comp., 2005, http://www.lix.polytechnique.fr/Labo/Regis.Dupont/preprints/Dupont_FastEvalMod.ps.gz.

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

[31] 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.

[32] 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.

[33] 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.

[34] A. ENGE. *The complexity of class polynomial computation via floating point approximations*, HAL-INRIA, n$^o$ 1040, INRIA, 2006, http://hal.inria.fr/inria-00001040.

[35] A. ENGE, P. GAUDRY. *A General Framework for Subexponential Discrete Logarithm Algorithms*, in "Acta Arithmetica", vol. 102, n$^o$ 1, 2002, p. 83–103.

[36] 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.

[37] 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.

[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, T. HOUTMANN, D. KOHEL, C. RITZENTHALER, A. WENG. *The p-adic method for genus 2*, Preprint, 2005, http://arxiv.org/abs/math.NT/0503148.

[43] P. GAUDRY, T. HOUTMANN, D. R. KOHEL, C. RITZENTHALER, A. WENG. *The 2-adic CM method for genus 2 with application to cryptography*, in "Advances in Cryptology – ASIACRYPT 2006", X. LAI, K. CHEN (editors), Lecture Notes in Comput. Sci., vol. 4284, Springer-Verlag, 2006, p. 114–129.

[44] 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.

[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.", May 2007, http://www.ams.org/mcom/0000-000-00/S0025-5718-07-02010-8/S0025-5718-07-02010-8.pdf.

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

[48] 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.

[49] 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.

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

[51] 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.

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

[53] J. MCKEE. *Speeding Fermat's Factoring Method*, in "Math. Comp.", vol. 68, n° 228, October 1999, p. 1729-1737.

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

[55] M. A. MORRISON, J. BRILLHART. *A method of factoring and the factorization of $F_7$*, in "Math. Comp.", vol. 29, n° 129, January 1975, p. 183-205.

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

[57] 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.

[58] E. TESKE. *An elliptic trapdoor system*, in "J. of Cryptology", vol. 19, n° 1, 2006, p. 115–133.