INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team tanc

Algorithmic number theory for cryptology

Saclay - Île-de-France

Theme : Algorithms, Certification, and Cryptography

Activity Report

2010

Table of contents

1. Team

Research Scientists

Daniel Augot [DR2 / Senior Researcher, Interim Team Leader, HdR]
Benjamin Smith [CR1 / Junior Researcher]

Faculty Member

François Morain [Team leader, Professor at École polytechnique, HdR]

Technical Staff

Jérôme Milan [Ingénieur CNRS]

PhD Students

Luca De Feo [École polytechnique since 2007-09-01, defended 2010-12-13]
Jean-François Biasse [DGA since 2007-09-01, defended 2010-09-20]
Morgan Barbier [École polytechnique since 2008-10-01]
Guillaume Quintin [DGA since 2009-10-01]

Post-Doctoral Fellow

Sorina Ionica [DGA since 2010-10-01]

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, and most notably the computational aspects of these objects, which appear as a substitute for modular arithmetic in new analogues of old-fashioned cryptography. One reason for this change is that we can achieve an equivalent security level with a much smaller key size. Our research contributes to the effort to find a diverse range of secure substitutes for the famous RSA (Rivest–Shamir–Adleman) cryptosystem, in case some attack appears and destroys the products that use 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 (re-)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: We tackle algorithmic problems involving efficiently computing group laws on Jacobians of curves, evaluating the cardinality of these objects, and studying the security of the discrete logarithm problem in such groups. These topics are crucial to the applicability of these objects 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.

- List Decoding of Algebraic codes Using List Decoding, one can fight adversarial noise, at the same level as Shannon limit for stochatsic noise. Daniel Augot defended his habilitation on this topic.
- Decoding algorithms for Algebraic Geometric codes: The algorithmic knowledge of TANC will be used to accelerate 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 also aim to promote the use of curve-based cryptography in new environments, such as *ad hoc* networks. We will also try to promote the use of AG codes, which are the coding-theoretic analogue of elliptic curves in cryptology.

2.3. Highlights

FMorain has improved its own primality proving record on ordinary numbers (more than 25000 decimal digits), a record announced during ECC2010.

Jean-François Biasse defended his PhD thesis, “Algorithmes sous-exponentiels pour les corps de nombres” on 20/09/2010. He is currently working with the MAGMA group in Sydney.

Luca De Feo successfully defended his PhD thesis, “Fast algorithms for towers of finite fields and isogenies”, on 13/12/2010. He is now working as a postdoctoral researcher at Rennes.

3. Scientific Foundations

3.1. General overview

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

However, modern networks are simply too large for the classical paradigm to remain efficient any longer. Hence the need for cryptography without prior contact. In theory, this is easy: find two algorithms E and D that are reciprocal (that is, $D(E(m)) = m$) 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 single user. When Alice wants to send an email message m to Bob, she uses his public key E to send him the encrypted message $E(m)$, which he can decrypt with the secret key D: we have thus achieved secret communication without a common secret key. (Of course, everything has to be presented in the modern language of complexity theory: E and D must be computable in polynomial time, while finding D from E alone without some secret knowledge should be possible only in, say, exponential time.) This simplified and somewhat idealized example is at the heart of asymmetric cryptology. Modern asymmetric cryptography provides not only secure communication channels but also 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 (such as ssh and ssl/tls).

Now, where do the hard problems behind encryption and decryption come from? Mostly from arithmetic, where we find problems such as the integer factorization and the discrete logarithm problem. It appears to be important to vary the groups which act as settings for concrete instances of the abstract hard problems, since this provides some bio-diversity which is key to resisting crypto-analytic attacks. The groups proposed include finite fields, modular integers, algebraic curves, and class groups. All of 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 for breaking records, whatever the subject is: constructing systems or breaking them. We have world-record computations in areas including primality proving, class polynomials, modular equations, computing cardinalities of algebraic curves, and discrete logarithms. This means writing programs and putting in all the work needed to support calculations that run for weeks or months. An important part of our task is now to transform record-breaking programs into programs to solve everyday cryptographic problems for current parameter sizes.

Certificates are another of our major concerns. By certificates, we mean efficiently verifiable proofs of the properties of the objects we build. While these certificates might be difficult to build, they are easy to check (by customers, for example). The traditional example is certificates for primality of prime numbers, introduced by Pratt in 1974. We know how to construct certificates for the important properties of 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, its discriminant with proven factorization, and the class number of the associated order). The theory is ready for this, and the algorithms are not out of reach. This approach must be extended to other curves; the theory is almost ready in several cases, but algorithms are still to be found. This is one of the main problems facing TANC.

The mathematics used in cryptology is becoming more and more complex (for example, consider recent algorithms based on p-adic cohomology). The new, more mathematically complex algorithms will remain mere theoretical curiosities if we do not implement them. For implementations, we need more and more evolved algorithmic primitives; currently, these may be available in very rare mathematical systems such as MAGMA. Once our 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 developed for our research (an old version of ECPP, some parts of discrete log computations, cardinality of curves) are now included in the MAGMA system, as a result of our collaboration with the Sydney group.

3.2. Algebraic curves over finite fields

One of the most common cryptographic protocols is Diffie–Hellman Key Exchange, which enables Alice and Bob to exchange 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; real-life protocols based on this need more security properties. Being unable to recover a from g^a (the Discrete Log Problem, or *DLP*) is fundamental to the security of the scheme, and groups for which the *DLP* is hard must be favored. Therefore, the choice of group G is crucial; TANC concentrates on groups derived from algebraic curves. These groups offer a very interesting alternative to finite fields: the *DLP* in a finite field can be broken by subexponential algorithms, while exponential time is required for an elliptic curve over the same field. Smaller keys can therefore be used in curve-based cryptosystems; this is very interesting from the point of view of limited-power devices.

In order to build a cryptosystem based on an algebraic curve over a finite field, one needs to efficiently compute the group law (and hence have a nice representation for elements of the Jacobian of the curve). Next, one must compute the cardinality of the Jacobian, so that we can find generators of the group. Once the curve is built, one needs to test its security, for example by determining the hardness of the *DLP* in its Jacobian.

3.2.1. Effective group laws

The curves that interest us are typically defined over a finite field $\mathrm{GF}(p^n)$, where p is the (prime) 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 over the preceding millennium. Adding two points is usually done using the so-called *chord-and-tangent* formulæ. When dealing with a genus g curve (the elliptic curve 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 now completed.

3.2.2. Cardinality

Once the group law is tractable, one has to find means of computing the cardinality of the group: this 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 currently known algorithm for computing the number of points of an elliptic curve over $\mathrm{GF}(p)$ is the Schoof–Elkies–Atkin algorithm. Thanks to the work of the project, 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 [64]). The current record for SEA was established by F. Morain in 2007 for a prime p of 2500 decimal digits (compared to 500dd back in 1995), using the work in [3] and in [10], in which a new approach to 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 current fastest algorithm, based on the arithmetic-geometric mean (AGM). Developed by R. Harley and P. Gaudry, it led to new world records. Then, P. Gaudry combined this method with other approaches to make it competitive for cryptographic sizes [63].

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 [65]. To get one step further, one needs to use genus 2 analogues of modular equations. After a theoretical study [66], 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 Monsky–Washnitzer cohomology. His algorithm was originally designed for $p > 2$. P. Gaudry and N. Gürel implemented this algorithm and extended it to superelliptic curves, thus 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 [61]). 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 [47]. Primes p around 10^9 are now doable.

3.2.3. Computing isogenies

The core of the Schoof–Elkies–Atkin (SEA) algorithm for computing cardinality of elliptic curves over large-characteristic finite fields consists in using the theory of isogenies to find small factors of division polynomials.

Isogenies are also a tool for understanding the difficulty of the Discrete Log problem among classes of elliptic curves [75]. Recently, there appeared suggestions to use isogenies in a cryptographic context, replacing the multiplication on curves by composition of isogenies [85], [83].

Algorithms for computing isogenies are very well known and widely used in the large characteristic case. When the characteristic is small, three algorithms exist: two due to Couveignes [51], [52], [79], and one due to Lercier [78].

3.2.4. The Discrete Logarithm Problem

The Discrete Logarithm Problem (DLP) is one of the major difficult problems upon which we build secure cryptosystems. It has essentially been proven equivalent to the computational Diffie–Hellman problem, which corresponds more closely to the actual security of many protocols. For an arbitrary group of prime order N, the DLP can be solved by a generic, exponential algorithm in $\Theta(\sqrt{N})$ group operations. For elliptic curves (setting aside some rare and easily avoidable instances), no faster algorithms are known.

For 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 [45], and A. Enge developed the first algorithm with a proven subexponential run time of $L(1/2)$ in [57]. Generalisations to other groups proposed for cryptography (in particular ideal class groups of imaginary quadratic number fields) are obtained by A. Enge and P. Gaudry in [6] and [56]. Proofs for arbitrary curves of large genus are given by J.-M. Couveignes [50] and F. Heß [72].

The existence of subexponential algorithms shows that high genus curves are less secure than low-genus curves (including elliptic curves) in cryptography. By analyzing the same algorithms differently, concrete recommendations for key lengths can be obtained, an approach introduced by P. Gaudry in [62] and pursued in [67]. 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 analyzed in [6], C. Diem has shown in [53] that non-hyperelliptic curves (of genus at least 3) are even less secure than hyperelliptic ones of the same genus. This effectively leaves only elliptic and low genus hyperelliptic curves as potential sources for public-key cryptosystems.

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 some useful properties are too rare to occur (suitability for pairings, for instance). In some cases, curves with special properties can be used. For example, curves with *complex multiplication* (in brief CM), have easily-computable cardinalities. For example, the elliptic curve by the equation $y^2 = x^3 + x$ over $GF(p)$ has cardinality $p + 1 - 2u$, when $p = u^2 + v^2$, and computing this u is easy.

The CM theory for genus 1 is well known, dating back to the middle of the nineteenth century (Kronecker, Weber, etc.). Its algorithmic aspects are also well understood; 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 since then by F. Morain. Though the decision problem ISPRIME? was shown to be in *P* (by the work of Agrawal, Kayal, and Saxena in 2002), practical primality proving for 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 for use in Identity Based Cryptosystems [55].

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 one hand, and A. Enge (together with R. Schertz) on the other, have developed the use of new class invariants characterizing CM curves. The union of these two families is currently the state of the art in the field (see [8]). More recently, 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 [58]. 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 [13] [81]), 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 Agrawal–Kayal–Saxena [77] has complexity $O((\log N)^{6+\epsilon})$, and has not been implemented so far; the best randomized version [46] reaches the same $O((\log N)^{4+\epsilon})$ bound but suffers from memory problems, and is not yet competitive. F. Morain implemented fastECPP, and was able to prove the primality of $10,000$ decimal digit numbers [13], as opposed to $5,000$ for the basic (historical) version. Continual improvements to this algorithm led to new records in primality proving, some of which were obtained with his co-authors J. Franke, T. Kleinjung and T. Wirth [60] who developed their own programs. F. Morain set the current world record to 20,562 decimal digits in early June 2006 (compared to 15,071 two years earlier). This record was made possible by using an updated MPI-based implementation of the algorithm, and distributing the 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 investigated the complexity of the evaluation of some modular functions and forms (such as the elliptic modular function j and the Dedekind eta function). 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 [22].

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

A. Enge has been able to analyse precisely the complexity of class polynomial computations via complex floating point approximations [5]. Using techniques from fast symbolic computation (multievaluation of polynomials) and results from R. Dupont's PhD thesis [54], 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 optimized algorithm based on Chinese remaindering in [2] 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 [2], A. Sutherland has come up with a new implementation of the Chinese remainder based algorithm that has led to new record computations [84]. 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.

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, proven the convergence of these sequences in a general setting, and determined the set of limits of such sequences in genus 2. In particular, he proved a theorem parametrizing the set of all possible limits of Borchardt sequences starting with a fixed 4-tuple. He developed an algorithm for the fast evaluation of theta constants in genus 2, and as a byproduct obtained 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).

3.4. Algebraic Geometry codes

There are many other applications of algorithmic methods for algebraic curves besides asymmetric cryptography. Daniel Augot plans to develop a new activity around algebraic geometry (AG) codes, a very powerful family of codes that often beat records for their parameters: they often offer the best correction capacity. The main topic of research is to accelerate the decoding algorithms of these codes, which have a slightly expensive cost [73]. A reference implementation would be of major interest, to help people compare AG codes with Reed–Solomon codes.

Guruswami and Sudan have obtained a breakthrough [70] for decoding AG codes with many errors. Still, there is no implementation available yet, 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. Communications

Clearly, our main field of applications is telecommunications. We participate in the protection of information. We are proficient on a theoretical level, and ready to develop applications using modern cryptographic techniques, with a main focus on elliptic curve cryptography and codes based on algebraic curves. One potential application is cryptosystems in environments with limited resources as smart cards, mobile phones, and *ad hoc* networks. For coding, we envisage developing algebraic codes for the erasure channel or distributed storage.

5. Software

5.1. ECPP

F. Morain has been continuously improving his primality proving algorithm called ECPP, originally developed in the early 1990s. Binaries for version 6.4.5 have been available since 2001 on his web page. Proving the primality of a 512 bit number requires less than a second on an average PC. His personal record is around $25,000$ decimal digits, with the fast version he started developing in 2003. All of the code is written in C, and based on the GMP package.

5.2. TIFA

In late 2005, we hired J. Milan as *ingénieur associé* to help us in developing and cleaning our programs. He first spent some time making a tour of publicly available implementations of the IEEE P-1363 cryptography standards. Following this study, it did not appear worthwhile to develop our own framework when others were approaching maturity and almost complete. He therefore switched to one of our other themes, namely writing integer factorization software for which the results can be certified.

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 [44] we are involved in, together with other teams including 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), which is asymptotically the fastest currently known integer factorization algorithm. 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 producing identity cards for elliptic curves, in order to select curves with the properties needed for cryptographic use. An identity card requires the knowledge of the factorization of the order of the curve (about 200 bits for cryptographic use).

Hence, J. Milan began the development of the so-called TIFA library (short for Tools for Integer FActorization) in 2006. TIFA is made up of a base library written in C99 using the GMP library, together with stand-alone factorization programs and a basic benchmarking framework to assess the performance of the relative algorithms.

TIFA has been continuously improved during the last few years. As of november 2009, TIFA includes the following algorithms :

- CFRAC (Continued FRACtion factorization [82])
- ECM (Elliptic Curve Method)
- Fermat (McKee's "fast" variant of Fermat's algorithm [80])
- SIQS (Self-Initializing Quadratic Sieve [49])
- SQUFOF (SQUare FOrm Factorization [69])

In early 2009, disappointing comparisons to other factorization tools (such as the ones provided by PARI/GP) prompted J. Milan to undertake a major rewrite of his SIQS implementation. Together with other optimizations throughout the code base, this effort led to dramatic improvements, making TIFA's SIQS more than twice as fast as PARI/GP's version. TIFA's SQUFOF and SIQS are now amongst the fastest available implementations. For tiny numbers (say between 100 to 160 bits), TIFA's SIQS may even be the fastest.

J. Milan still plans to maintain and improve the library, particularly its ECM implementation which is, now, the only significant part of the software which is really behind the competition.

So far, TIFA has been kept internal to the TANC team and CADO project. Recently, we have received several requests from the community asking for access to this library. Consequently, we are in the process of making it public under an open source license (most probably the Lesser General Public License version 2.1 or higher). We plan to have it available before the end of the year, or at worst, in early 2010.

5.3. FAAST

The FAAST library is developed in C++ by L. De Feo and makes use of the NTL library. It implements the algorithms presented in [4], plus other algorithms needed by the author for his research on explicit isogenies.

Version 0.2.0, released on July 11 2009, is available at http://www.lix.polytechnique.fr/Labo/Luca.De-Feo/FAAST/. The source code is distributed under the General Public License version 2 or higher.

FAAST is a very efficient library for lattices of extensions of finite fields. Our aim is to add support for arbitrary finite fields, making it an essential building block for efficient computer algebra systems.

6. New Results

6.1. Algebraic curves over finite fields

6.1.1. Isogenies and Point Counting

Participants: François Morain, Luca De Feo, Benjamin Smith, Sorina Ionica.

Together with A. Bostan, B. Salvy (from projet ALGO), and É. Schost, F. Morain gave quasi-linear algorithms for computing the explicit form of an isogeny between two elliptic curves, another important block in the SEA algorithm [3]. This article contains a survey of previous methods, all applicable in the large characteristic case. Joux and Lercier recently announced a p-adic approach for computing isogenies in all characteristic with the same complexity, 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. In 2009 L. De Feo and É. Schost gave new asymptotically fast algorithms for arithmetic in Artin–Schreier towers [4]. The algorithms have been packaged in the C++ library FAAST and served as a basis for a new efficient implementation of Couveignes' algorithm. Integration with F. Morain's implementation of SEA is in progress. An article is in preparation giving the details of the implementation and the improvements to the original algorithm.

Recently, B. Smith has given a series of new constructions of families of isogenies of Jacobians of high-genus curves; the existence of these families is remarkable. An article exhibiting twelve families of higher-genus hyperelliptic curves appeared in the proceedings of AGCT 12 [29]. An article describing six infinite series of hyperelliptic and non-hyperelliptic families (each giving isogenies in arbitrarily high dimension) has been accepted for publication [43].

A collaboration between B. Smith, P. Gaudry (CARAMEL), and D. Kohel (Marseille) has resulted in computations smashing the previous records for point counting on certain genus 2 curves in large characteristic. The prior state of the art computed cardinalities of a 127-bit Jacobian in around one CPU month; we can now compute a kilobit Jacobian with the same effort. This work renders cardinality computations for genus 2 curves over cryptographic-sized prime fields truly practical for the first time. We announced these results at a number of workshops and seminars this year, including the "Counting points: theory, algorithms, and practice" meeting at the CRM, Université de Montréal, in April 2010; an article describing the new algorithm, and families of applicable curves, is in preparation.

6.1.2. Discrete logarithms on curves

Participants: Jean-François Biasse, Benjamin Smith.

An extended version of B. Smith's 2008 work on polynomial-time reductions 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 [53] can solve the discrete logarithm problem in time $\widetilde{O}(q)$, a significant improvement over the previous best known $\widetilde{O}(q^{4/3})$ algorithm for solving hyperelliptic genus 3 discrete logarithms due to P. Gaudry, E. Thomé, N. Thériault, and C. Diem [67]) has now appeared in the Journal of Cryptology [14].

6.2. Complex multiplication

Participant: François Morain.

Morain and Enge have contributed to the study of generalized Weber functions, enabing a partial classification for some cases [41].

Morain has been investigating (with É. Brier) the properties of modular curves $X_0(N)$ to be able to introduce new optimal class invariants. This led him to begin the classification of such important curves and to compute new modular equations [42].

6.3. Algebraic codes

Participants: Daniel Augot, Morgan Barbier.

6.3.1. List decoding of Reed–Solomon codes

This is a new activity of the TANC project-team, whose aim is to accelerate decoding algorithms for 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 [17]. 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.

6.3.2. List decoding of Algebraic Geometry codes

This is also a new activity for the TANC project team, started with the arrival of Guillaume Quintin, a new PhD student, supervised by Daniel Augot and Grégoire Lecerf (from the university of Versailles Saint-Quentin). These AG codes are a generalization of Reed–Solomon codes. G. Quintin did a first implementation of the factorisation step in MAGMA, to understand the algorithms and the needed material. He is starting to rewrite the algorithm within the MATHEMAGIX framework.

6.3.3. List decoding of binary codes

Another new topic that began 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 [86], 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; we intend to apply Wu's algorithm in steganography, using the ideas of Fontaine and Galand [59]. They used Reed–Solomon codes, and it seems very natural to use the same ideas with BCH codes. Implementing Wu's algorithm and applying it to steganography is the plan of Barbier's thesis.

If the number of errors in a received word is less than the code's error correction capacity, the decoding algorithm is guaranteed to return a single codeword. This property led to the term *unique decoding*, which has been (and still mostly is) the standard decoding method. However, in the last decade much attention has been given to so-called *list decoding* methods which can correct far more errors, at the expense of losing the uniqueness of the decoded word.

While the concept of list decoding code dates back to the 1950s, the first interesting algorithm only appeared in 1995, when Madhu Sudan introduced a list decoding algorithm for Reed–Solomon codes that could correct up to $1-\sqrt{2R}$ errors, where $R=\frac{k}{n}$ is the code rate. Building upon this work, Sudan and his student Venkatesan Guruswami then designed an improvement to Sudan's algorithm correcting $1-\sqrt{R}$ errors. Since then, a few other algorithms were proposed but Guruswami–Sudan is still considered to be the reference for list decoding.

As previously mentioned, list decoding trades the uniqueness of the corrected codeword for larger correction capabilities. Needless to say, if more errors are allowed, the list of returned codeword candidates will be larger. An important bound in list decoding is due to Johnson. Basically, if the number n_e of errors allowed is less than the Johnson bound $J_q(n,d)$, then the size of the candidate list will grow polynomially with n_e. For a linear code $\mathcal{C}$ defined over $\mathbb{F}_q$, of length n, dimension k and minimal distance d, the Johnson bound is given by

$$J_q(n,d)=n\frac{q-1}{q}\left(1-\sqrt{1-\frac{q}{q-1}\frac{d}{n}}\right).$$

Traditionally, we distinguish the binary codes, defined over $\mathbb{F}_2$, from the general case. For binary codes, the Johnson bound takes the simpler form

$$J_2(n,d) = \frac{n}{2} - \frac{n}{2}\sqrt{1 - \frac{2d}{n}}.$$

In the general case, provided $q/(q-1) \approx 1$, we approximate $J_q(n,d)$ by

$$J(n,d) = n - n\sqrt{1 - \frac{d}{n}}.$$

The Johnson bound for binary curves is more interesting, since we are able to correct more errors for a given length and distance than in the general case.

Daniel Augot, Morgan Barbier and Alain Couvreur reach such a bound, better than Bernstein's [32], for the classical Goppa codes.

6.3.4. Homomorphic encryption

Gentry's breakthrough paper [68] has realized *fully homomorphic encryption*, albeit in a quite theoretical way. The defining property of these schemes is that operations on the ciphertexts correspond to the same operations on the plaintext. This enables powerful applications, including querying encrypted databases. But Gentry's scheme, although widely publicised, appears to be quite unpractical, since it implies huge ciphertexts.

Daniel Augot, Ludovic Perret, and Frederik Armknecht have devised a code-based homomorphic encryption scheme based on evaluation codes, which has been given a particular instance with q-ary Reed–Muller codes. Although our scheme is secret-key, it still enables the desirable applications envisioned by Gentry, and is much more efficient with respect to ciphertext size and computional complexity of encryption operations. A paper has been submitted to the FSE 2011 conference [24].

6.4. Number fields

Participant: Jean-François Biasse.

Jean-François Biasse has made practical improvements to the sieving-based algorithm of Jacobson [74] for computing the group structure of the ideal class group of an imaginary quadratic number field. These improvements, based on the use of large prime variants combined with proper structured gaussian elimination, led to the computation of the structure of a class group corresponding to a number field with a 110-digit discriminant (whereas older techniques were limited to 90-digit discriminants). This work has now appeared in the journal Advances In Mathematics of Communications [19].

Biasse has also determined a class of number fields for which the ideal class group, the regulator, and a system of fundamental units of the maximal order can be computed in subexponential time $L(1/3, O(1))$ (whereas the best previously known algorithms have complexity $L(1/2, O(1))$). This class of number fields is analogous to the class of curves described in [7] (cf. 6.1 above). The article [33] has been submitted to *Mathematics of Computation*.

In collaboration with Jacobson, Biasse described in [25] improvements to the sieving methods for ideal class group, regulator and fundamental unit computation. These improvements lead to a significant speed-up over the previous state of the art, and the computation of the regulator of a number field of a 110 digit discriminant, whereas the previous record was 100 digits.

In collaboration with Jacobson and Sylvester [26], Biasse improved the algorithms for sloving the discrete logarithm problem and the principal ideal problem which are involved in the design of the cryptosystems based on number fields. They assessed the impact of these improvements on the security of theses cryptosystems and provided estimates on the size of the keys required to ensure a level of security equivalent to the recommendations of the NIST.

6.5. Automatic transposition of programs

Participant: Luca De Feo.

The transposition principle roughly says that any matrix-vector product can be computed using the same number of operations as the corresponding transposed matrix-vector product. The application of this principle to computer programs is a topic of active research in computer algebra [76], [71], [48]. Luca De Feo and Éric Schost [21] have shown that automatic transposition of suitably annotated multilinear programs is possible, and are now implementing a compiler for a domain specific language called `transalpyne`.

7. Contracts and Grants with Industry

7.1. Contracts with Industry

- A GEMPLUS contract corresponds to É. Brier's thesis on the use of (hyper-)elliptic curves in cryptology.
- Daniel Augot is in discussion with MassiveRand, an SME providing random bits at high rate, in order to provide Rabin's HyperEncryption, which is provably secure.

8. Other Grants and Activities

8.1. Regional Initiatives

- DIGITEO have contributed the operational funding for the project AMIGA (Advanced Methods for Isogeny Graph Analysis), with B. Smith as the scientific leader of the project. On a national level, the DGA have contributed a postdoctoral salary to the project (see National Initiatives).

8.2. National Initiatives

- The DGA have funded a postdoctoral researcher's salary for Sorina Ionica, allowing her to join TANC for one year as a postdoctoral researcher within the project AMIGA.
- A short one-year teamwork between the INRIA Saclay project-teams TANC and Hipercom@LIX was initiated in January 2008 as part of the so-called Cryptonet OMT (Opération de Maturation Technologique). The goal of this joint effort, mainly financed by the Digiteo foundation, was to present a proof-of-concept of an hardened, more robust OLSRv2 ad hoc network protocol. In early 2010, T. Clausen, U. Herberg and J. Milan submitted an article as a follow-up to this Cryptonet project. This paper was accepted and presented by H. Herberg at the iTAP 2010 conference [27].

8.3. European Initiatives

- Procope PCH Hubert Curien with Ulm Universität.

9. Dissemination

9.1. Animation of the scientific community

- Daniel Augot is Membre du comité scientifique du séminaire CCA.
- Benjamin Smith organised the poster session at ANTS-X (10th international Algorithmic Number Theory Symposium) in Nancy (July 19-23, 2010).

9.2. Teaching

François Morain is in charge of the MPRI 2.12.2 course *Algorithmes arithmétiques pour la cryptologie*, and gave 5 lectures in it in 2010.

Daniel Augot gave lectures (24h00) on algebraic coding theory in the MPRI at the Master 2 level.

Benjamin Smith taught the module on elliptic curve cryptography and pairings in the MPRI Master 2 course *Cryptologie*, and took TDs for the course “Les bases de la programmation et de l’algorithmique” at the École polytechnique.

Luca De Feo was TA for the course “Programmation Web” in the first year of the Licence d’Informatique at Paris VII.

Jean-François Biasse was TA for the courses “Introduction to C++”, “Numerical Analysis”, and “Probability” at the École polytechnique.

9.3. Seminars and talks

- B. Smith presented an accelerated point-counting algorithm for genus 2 curves with explicit endomorphisms in the “Counting points: theory, algorithms, and practice” meeting at the CRM, Université de Montréal, in April 2010, and also at Téécom ParisTech.
- B. Smith gave a talk on cryptographic aspects of genus 2 curves in the CCA seminar (Codage, Cryptologie, Algorithmes) in April 2010.
- B. Smith gave a talk on families of explicitly isogenous Jacobians of high genus curves in the Algebra and Number Theory Seminar at the Université de Franche-Comté, Besançon, in February 2010.
- Daniel Augot gave a one hour talk « Vers de bons codes sur le corps à deux éléments », at « journées de la SMF », June 2010, Paris.
- Daniel Augot gave a talk on decoding for the Lee metric at the Shannon Institute, Dublin, and also at Télécom ParisTech.
- François Morain was invited speaker in the ECC2010 conference celebrating the 25th anniversary of elliptic curve in cryptology, at MSR (Redmond, October 18-22).
- Morgan Barbier made a presentation entitled “Introduction to the list decoding” at the University of Toulon at January 26th.
- Morgan Barbier made a presentation entitled “A new list decoding for the Reed-Solomon and BCH codes” at the University of Toulon (January 26).
- Morgan Barbier made a presentation entitled “On linear codes for the syndrome coding problem” at the Soria Summer school (July 14).
- Morgan Barbier gave a talk on “A new class of codes for the maximum-likelihood decoding problem”[30] at YACC (Yet Another Conference on Cryptography) (October 6).
- Guillaume Quintin gave a talk on “List decoding of algebraic geometric codes” at the Soria Summer school (July 12).
- Luca De Feo presented the paper “`transalpyne`: a language for automatic transposition” at the PLMSS conference (part of the CICM joint conference in CNAM, Paris) in July.

9.4. Vulgarization and Summer schools

- F. Morain was invited to the Festival PariScience in October 2010, to participate in a debate following a movie on the Riemann Hypothesis.
- Daniel Augot gave three hours of lectures on algebraic codes at the Journées Nationales du Calcul Formel in Luminy, and produced notes [23].
- Daniel Augot gave a popular science seminar on Coding Cryptography and Steganography for Versailles High School Math Teachers, and also for Polytechnique’s students.

9.5. Program Committees

- Daniel Augot is member of the program committee of PQ Crypto 2010, of WAIFI 2010, and of PASCO 2010.
- François Morain was co-head of the ANTS-IX conference (together with G. Hanrot), which took place in Nancy (July 19-23, 2010); this led to the Springer Volume [31].

9.6. Thesis committees

- Daniel Augot was reviewer of Thomas Roche's PhD Thesis "Dimensionnement et intégration d'un chiffre symétrique dans le contexte d'un système d'information distribué de grande taille", defended in Grenoble on January 29th, 2010.
- Daniel Augot was reviewer (with Caroline Fontaine) of Cyril Bazin's PhD Thesis "Tatouage de données géographiques et généralisation aux données devant préserver des contraintes", defended in Caen on January 19th, 2010.
- Daniel Augot was reviewer of Alexander Soro's PhD thesis "Mécanismes de fiabilisation pro-actifs", defended in Toulouse on December 3rd, 2010.
- Daniel Augot was reviewer of Amine Bouabdallah's PhD thesis "Contributions à la fiabilisation du transport video", defended in Toulouse on December 3rd, 2010.
- Daniel Augot was reviewer of Kristian Brander's PhD Thesis "Interpolation and List Decoding of Algebraic Codes", defended in Denmark, March 24th 2010.
- Daniel Augot was member of the thesis committees for Bhaskar Biswas (10/01/2010), Stéphane Manuel (11/23/2010), Maxime Côte (03/12/2010), Lionel Chaussade (11/22/2010) Thesis Committee (03/22/2010).
- Daniel Augot was a member of Françoise Lévy-dit-Véhel's HdR Committee, defended on September 10th, 2010.
- Benjamin Smith was a member of Sorina Ionica's Ph.D. thesis committee, defended on May 14th, 2010.
- F. Morain was the president of the defense committee for D. Robert (21/07/2010).

9.7. Research administration

- Daniel Augot is Responsable du suivi doctoral du CRI Saclay Île-de-France.
- Daniel Augot is Membre de la commission scientifique du CRI Saclay Île-de-France.
- Daniel Augot was Membre du comité de sélection de Paris 6 (deux postes).

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.", 2005, vol. 74, p. 389–410, http://hal.inria.fr/inria-00071967.

[2] J. Belding, R. Bröker, A. Enge, K. Lauter. *Computing Hilbert class polynomials*, in "Algorithmic number theory", Berlin, Lecture Notes in Comput. Sci., Springer, 2008, vol. 5011, p. 282–295.

[3] A. Bostan, F. Morain, B. Salvy, É. Schost. *Fast algorithms for computing isogenies between elliptic curves*, in "Math. Comp.", 2008, vol. 77, n^{o} 263, p. 1755–1778, http://dx.doi.org/10.1090/S0025-5718-08-02066-8.

[4] L. DE FEO, É. SCHOST. *Fast Arithmetics in Artin-Schreier towers*, in "ISSAC 2009", 2009, p. 121-134.

[5] A. ENGE. *The complexity of class polynomial computation via floating point approximations*, in "Mathematics of Computation", 2008, vol. 78, p. 1089-1107, http://hal.inria.fr/inria-00001040/PDF/class.pdf.

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

[7] 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., Springer-Verlag, 2007, vol. 4515, p. 379–393, http://hal.inria.fr/inria-00135324.

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

[9] A. ENGE, R. SCHERTZ. *Constructing elliptic curves over finite fields using double eta-quotients*, in "Journal de Théorie des Nombres de Bordeaux", 2004, vol. 16, p. 555–568, http://jtnb.cedram.org/jtnb-bin/fitem?id=JTNB_2004__16_3_555_0.

[10] 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.

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

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

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

[14] B. SMITH. *Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves*, in "J. of Cryptology", 2009, vol. 22, n^o 4, p. 505-529.

Publications of the year

Doctoral Dissertations and Habilitation Theses

[15] J.-F. BIASSE. *Subexponential algorithms for number fields*, École polytechnique, 2010.

[16] L. DE FEO. *Algorithmes Rapides pour les Tours de Corps Finis et les Isogénies*, Ecole Polytechnique X, 12 2010, http://tel.archives-ouvertes.fr/tel-00547034/en/.

Articles in International Peer-Reviewed Journal

[17] D. AUGOT, C. GENTNER, A. ZEH. *A Berlekamp-Massey Approach for the Guruswami-Sudan Decoding Algorithm for Reed-Solomon Codes*, in "IEEE Transactions on Information Theory", submitted 2010.

[18] M. BARBIER. *A New Class of codes for the Maximum-Likelihood Decoding Problem*, in "Cryptography and Communications", submitted 2010, 10 pages.

[19] J.-F. BIASSE. *Improvements in the computation of ideal class groups of imaginary quadratic number fields*, in "Advances in Mathematics of Communications", 2010, vol. 4, n^{o} 2, p. 141-154, http://hal.inria.fr/inria-00397408/.

[20] L. DE FEO. *Fast algorithms for computing isogenies between ordinary elliptic curves in small characteristic*, in "Journal of Number Theory", Aug 2010, In Press [*DOI :* 10.1016/J.JNT.2010.07.003], http://hal.inria.fr/hal-00505798/en.

[21] L. DE FEO, É. SCHOST. *transalpyne: a language for automatic transposition*, in "ACM SIGSAM Bulletin", Jul 2010, vol. 44, n^{o} 1/2, p. 59-71 [*DOI :* 10.1145/1838599.1838624], http://hal.inria.fr/hal-00505809/en.

[22] R. DUPONT. *Fast evaluation of modular functions using Newton iterations and the AGM*, in "Math. Comp.", 2010, To appear, http://www.lix.polytechnique.fr/Labo/Regis.Dupont/preprints/Dupont_FastEvalMod.ps.gz.

Articles in Non Peer-Reviewed Journal

[23] D. AUGOT. *Les codes algébriques principaux et leur décodage*, in "Les cours du CIRM", may 2010, vol. 1, p. 31-74, http://hal.inria.fr/inria-00543322/en/.

International Peer-Reviewed Conference/Proceedings

[24] F. ARMKNECHT, D. AUGOT, L. PERRET, A.-R. SADEGHI. *Algebraically Homomorphic Encryption from Evaluation Codes*, in "FSE 2011", 2011, submitted.

[25] J.-F. BIASSE, M. JACOBSON. *Practical improvements to class group and regulator computation of real quadratic fields*, in "Algorithmic Number Theory Symposium – ANTS IX", Berlin, G. HANROT, F. MORAIN, E. THOMÉ (editors), Lecture Notes in Computer Science, Springer-Verlag, 2010, vol. 6197, p. 50–65, http://hal.inria.fr/inria-00477896/.

[26] J.-F. BIASSE, M. JACOBSON, A. SILVESTER. *Security estimates for quadratic field based cryptosystems*, in "Australasian Conference in Information Security and Privacy – ACISP 2010", Berlin, P. HAWKES, R. STEINFELD (editors), Lecture Notes in Computer Science, Springer-Verlag, 2010, vol. 6168, p. 233–247, http://hal.inria.fr/inria-00477949/.

[27] U. HERBERG, T. H. CLAUSEN, J. MILAN. *Digital Signatures for Admittance Control in the Optimized Link State Routing Protocol Version 2*, in "Internet Technology and Applications, 2010 International Conference on", August 2010, http://dx.doi.org/10.1109/ITAPP.2010.5566285.

[28] S. IONICA, A. JOUX. *Pairing Computation on Elliptic Curves with Efficiently Computable Endomorphism and Small Embedding Degree*, in "Pairing-Based Cryptography – Pairing 2010", M. JOYE, A. MIYAJI, A. OTSUKA (editors), Lecture Notes in Comput. Sci., Springer, 2010, vol. 6487, p. 435-449.

[29] B. SMITH. *Families of Explicit Isogenies of Hyperelliptic Jacobians*, in "Arithmetic, Geometry, Cryptography and Coding Theory 2009 Contemporary Mathematics", Luminy France, D. KOHEL, R. ROLLAND (editors), Contemporary Mathematics, American Mathematical Society, 2010, vol. 521, p. 121-144, http://hal.inria.fr/inria-00420605/.

Workshops without Proceedings

[30] M. Barbier. *New Set of Codes for the Maximum-Likelihood Decoding Problem*, in "Yet Another Conference on Cryptography", France Porquerolles, Oct 2010, http://hal.inria.fr/inria-00534726/en.

Books or Proceedings Editing

[31] G. Hanrot, F. Morain, E. Thomé (editors). *Algorithmic Number Theory*, Lecture Notes in Comput. Sci., Springer-Verlag, 2010, vol. 6197, 9th International Symposium, ANTS-IX, Nancy, France, July 2010, Proceedings.

Research Reports

[32] D. Augot, M. Barbier, A. Couvreur. *List-decoding of binary Goppa codes up to the binary Johnson bound*, INRIA, 12 2010, n$^{\text{o}}$ RR-7490, http://hal.inria.fr/inria-00547106/en/.

[33] J.-F. Biasse. *An L(1/3) algorithm for ideal class group and regulator computation in certain number fields*, HAL-INRIA, 2010, n$^{\text{o}}$ 440223, http://hal.inria.fr/inria-00440223/.

[34] T. H. Clausen, U. Herberg, J. Milan. *Digital Signatures for Admittance Control in the Optimized Link State Routing Protocol version 2*, INRIA, Feb 2010, n$^{\text{o}}$ RR-7216, http://hal.inria.fr/inria-00460057/en.

Other Publications

[35] A. Couvreur. *Differential Approach for the Study of Duals of Algebraic-Geometric Codes on Surfaces*, Preprint, http://hal.inria.fr/inria-00541894/en.

[36] A. Couvreur. *The dual minimum distance of arbitrary dimensional algebraic-geometry codes*, Une partie de ce travail de recherche a été effectuée lorsque l'auteur de l'article était membre de l'institut de mathématiques de Luminy., http://hal.inria.fr/inria-00540022/en.

[37] A. Couvreur. *Construction of Rational Surfaces Yielding Good Codes*, 2010, 18 pages, 7 figures, http://hal.archives-ouvertes.fr/inria-00547454.

[38] A. Couvreur. *Differential approach for the study of duals of algebraic-geometric codes on surfaces*, 2010, 20 pages, http://hal.inria.fr/inria-00510725/en.

[39] L. De Feo. *On computing isogenies of unknown degree*, Aug 2010, http://hal.inria.fr/hal-00505791/en.

[40] L. De Feo, É. Schost. *Fast Arithmetics in Artin-Schreier Towers over Finite Fields*, 2010, Preprint, http://hal.inria.fr/hal-00505799/en.

[41] A. Enge, F. Morain. *Generalised Weber Functions. I*, Preprint, http://hal.inria.fr/inria-00385608/en/.

[42] F. Morain. *Modular equations for some η-products*, December 2010, In preparation.

[43] B. Smith. *Families of explicitly isogenous Jacobians of variable-separated curves*, 14K02; 11G30; 11Y99, http://hal.inria.fr/inria-00516038/.

[44] THE CADO TEAM. *CADO — Number field sieve: distribution, optimization*, 2010, http://cado.gforge.inria.fr/.

References in notes

[45] 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., Springer-Verlag, 1994, vol. 877, p. 28–40.

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

[47] 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., Springer-Verlag, 2004, vol. 2948, p. 40–58, http://www.lix.polytechnique.fr/Labo/Pierrick.Gaudry/publis/cartierFq7.ps.gz.

[48] A. BOSTAN, G. LECERF, É. SCHOST. *Tellegen's principle into practice*, in "ISSAC '03: Proceedings of the 2003 international symposium on Symbolic and algebraic computation", New York, NY, USA, ACM, 2003, p. 37–44, http://dx.doi.org/10.1145/860854.860870.

[49] S. CONTINI. *Factoring integers with the self-initializing quadratic sieve*, 1997, http://www.crypto-world.com/documents/contini_siqs.pdf.

[50] 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.

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

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

[53] 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, Springer-Verlag, 2006, vol. 4076, p. 543–557.

[54] R. DUPONT. *Moyenne arithmético-géométrique, suites de Borchardt et applications*, École polytechnique, 2006.

[55] R. DUPONT, A. ENGE, F. MORAIN. *Building curves with arbitrary small MOV degree over finite prime fields*, in "J. of Cryptology", 2005, vol. 18, n^{o} 2, p. 79–89, http://hal.inria.fr/inria-00386299.

[56] 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, Kluwer Academic Publishers, 2001, vol. 3, p. 133–146.

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

[58] 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., Springer-Verlag, 2003, vol. 2643, p. 254–264, 15th International Symposium, AAECC-15, Toulouse, France, May 2003, Proceedings.

[59] 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, Springer Berlin / Heidelberg, 2007, n^o 4567, p. 130–144.

[60] 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., Springer-Verlag, 2004, vol. 3076, p. 194–207, 6th International Symposium, ANTS-VI, Burlington, VT, USA, June 2004, Proceedings.

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

[62] 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., Springer-Verlag, 2000, vol. 1807, p. 19–34.

[63] 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., Springer–Verlag, 2002, vol. 2501, p. 311–327.

[64] 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 [*DOI :* 10.1145/1145768.1145791], http://hal.inria.fr/inria-00001009.

[65] 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., Springer-Verlag, 2004, vol. 3027, p. 239–256, http://www.lix.polytechnique.fr/Labo/Pierrick.Gaudry/publis/secureg2.ps.gz.

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

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

[68] C. GENTRY. *On Homomorphic Encryption over Circuits of Arbitrary Depth*, in "41st ACM Symposium on Theory of Computing (STOC 2009)", 2009.

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

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

[71] G. HANROT, M. QUERCIA, P. ZIMMERMANN. *The Middle Product Algorithm I*, in "Applicable Algebra in Engineering, Communication and Computing", March 2004, vol. 14, n^o 6, p. 415–438, http://dx.doi.org/10.1007/s00200-003-0144-2.

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

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

[74] M. JACOBSON. *Subexponential Class Group Computation in Quadratic Orders*, Technische Universität Darmstadt, Darmstadt, Germany, 1999.

[75] 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.

[76] E. KALTOFEN. *Challenges of Symbolic Computation: My Favorite Open Problems*, in "Journal of Symbolic Computation", June 2000, vol. 29, n^o 6, p. 891–919, http://dx.doi.org/10.1006/jsco.2000.0370.

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

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

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

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

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

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

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

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

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

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