IN PARTNERSHIP WITH:
CNRS

Ecole Polytechnique

Activity Report 2011

Project-Team TANC

Algorithmic number theory for cryptology

IN COLLABORATION WITH: Laboratoire d'informatique de l'école polytechnique (LIX)

RESEARCH CENTER
Saclay - Île-de-France

THEME
Algorithms, Certification, and Cryptography

Table of contents

Project-Team TANC

Keywords: Cryptography, Computer Algebra, Complexity, Algorithmic Numbers Theory, Error Detection And Correction, Security

1. Members

Research Scientists

Daniel Augot [DR2 / Senior Researcher, Team Leader, HdR]
Alain Couvreur [CR1 / Junior Researcher]
Benjamin Smith [CR1 / Junior Researcher, Responsable Permanent]

Faculty Member

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

Technical Staff

Jérôme Milan [CNRS Engineer]

PhD Students

Morgan Barbier [École polytechnique, 2008-10-01 to 2011-12-02]
Cécile Gonçalves [École polytechnique / DGA since 2011-10-1]
Guillaume Quintin [DGA since 2009-10-01]
Alexander Zeh [Ulm Universität, since 2010-05-1]

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 the 10th of March 2003.*

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 with efficient programming. Our main area of competence and interest is that of algebraic curves over finite fields, and most notably their computational aspects; these objects 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 global search for 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. The theory of curves over finite fields is also essential in the field of AG codes, and the algorithmic aspects of curves and their Jacobians are important for good implementations and analysis.
- 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 the Shannon limit for stochastic noise.
- Decoding algorithms for Algebraic Geometric codes: We use our algorithmic knowledge 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 our project-team name suggests, 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

BEST PAPER AWARD :
[26] **ASIACRYPT 2011**. P. GAUDRY, D. KOHEL, B. SMITH.

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.

We therefore need cryptography *without* prior contact. In theory, this is simple: 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 integer factorization and the discrete logarithm problem (DLP). 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 with generator g, Alice sends g^a for a random a to Bob, and Bob responds with g^b for a random 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. The difficulty of recovering 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, if frequently changing the group is imperative in applications, then this computation has to be done as fast as possible.

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 [49]), see also [3] and in [10], in which a new approach to eigenvalue computation is described and proven. Note that A. Sutherland now detains the record in computations using a new algorithm for computing modular polynomials.

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 [48].

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 [50]. To get one step further, one needs to use genus 2 analogues of modular equations. After a theoretical study [51], they are now investigating the practical use of these equations, finally leading to [52].

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 [46]). 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 [34]. 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 [58]. Recently, there appeared suggestions to use isogenies in a cryptographic context, replacing the multiplication on curves by composition of isogenies [67], [65].

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 [37], [38], [61], and one due to Lercier [60].

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 [32], and A. Enge developed the first algorithm with a proven subexponential run time of $L(1/2)$ in [43]. 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 [42]. Proofs for arbitrary curves of large genus are given by J.-M. Couveignes [36] and F. Heß [56].

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 [47] and pursued in [53]. 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 [39] 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 [41].

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 [44]. 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] [63]), 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 [59] has complexity $O((\log N)^{6+\epsilon})$, and has not been implemented so far; the best randomized version [33] 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 [45] 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.

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 [40], 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 [66]. 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. These algebraic geometry (AG) codes form 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 [57]. 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 [55] 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, the main problem is find a reasoneable complexity for these algorithms. 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 publicly available packages (GMP, mpfr, mpc, mpfrcx).

5.2. SEA

Together with E. Schost and L. DeFeo, F. Morain has developed a new implementation of the SEA algorithm that computes the cardinality of elliptic curves over finite fields (large prime case, case $p = 2$). It uses NTL and includes the more recent algorithms for solving all subtasks. The large prime case is relevant to cryptographical needs. The $p = 2$ case, though not directly useful, is a good testbed for the FAAST program of LDeFeo (see 5.4). This program forms a `gforge` project.

5.3. TIFA

The TIFA library (short for Tools for Integer FActorization) was initially developed in 2006 and has been continuously improved during the last few years. 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 each algorithm.

As of november 2011, the library includes the following algorithms:

- CFRAC (Continued FRACtion factorization [64])
- ECM (Elliptic Curve Method)
- Fermat (McKee's "fast" variant of Fermat's algorithm [62])
- SIQS (Self-Initializing Quadratic Sieve [35])
- SQUFOF (SQUare FOrm Factorization [54])

The complete TIFA package has been registered at the French Agency for Software Protection (APP – http://app.legalis.net/) on June, 1st 2011 with the Inter Deposit Digital Number:

`IDDN.FR.001.220019.000.S.A.2011.000.31235.`

It is now available online at http://www.lix.polytechnique.fr/Labo/Jerome.Milan/tifa/tifa.xhtml and distributed under the Lesser General Public License, version 2.1 or later.

5.4. 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.

5.5. Quintix

The Quintix library is a Mathemagix package available at http://www.mathemagix.org/www/main/index.en.html. It is developed in C++ within the Mathemagix computer algebra system. It implements basic arithmetic for Galois rings and their unramified extensions, basic functions for the manipulation of Reed-Solomon codes and the complete Sudan list-decoding algorithm. It also implements the root-finding algorithms presented in [30]. The source code is distributed under the General Public License version 2 or higher.

Quintix is a very efficient library for Galois rings, extensions of Galois rings and root-finding in Galois rings.

5.6. APIP

As part of his activity in the PACE ANR, J. Milan completed, under the supervision of A. Enge, the development of APIP (Another Pairings Implementation in PARI), a PARI/GP module to compute state-of-the-art cryptographic pairings over elliptic curves. This module was intended to be an experimental framework for comparing the performances of the main cryptographic pairings with an emphasis on the standard 128, 192 and 256 bit high security levels.

APIP implements the Tate, Weil, ate and twisted ate pairings together with some optimal variants of the ate and twisted ate pairings for some elliptic curve families. Due to its very flexible architecture, it makes it easy to select several algorithm variants for each step of a pairing computation for a finer analysis.

Due to its emphasis on pairings for cryptographic purposes only, it is doubtful that the APIP module will be integrated in the upstream PARI/GP code base. We hope to be able to distribute APIP as an independent module in the near future, ideally under an open-source licence.

6. New Results

6.1. Point counting

In joint work with Pierrick Gaudry (CARAMEL) and David Kohel (Marseille), B. Smith developed an accelerated Schoof-type point counting algorithm for genus 2 curves with efficiently computable real multiplication endomorphisms. This project has made the computation of cryptographic-sized group orders practical for curves of genus 2 over prime finite fields. Going way beyond the current cryptographic range, the algorithm has been used to compute the group order of a 1024-bit Jacobian (smashing the previous 256-bit record of Gaudry and Schost). The article describing this algorithm has been awarded the Best Paper prize at ASIACRYPT 2011 [26], and an extended version has been invited for submission to Journal of Cryptology (the leading journal in the field).

6.2. Complex multiplication

F. Morain has been investigating new invariants for building class polynomials with small coefficients. This is still work in progress, though advertised in some talks of his.

6.3. Steganography

D. Augot, M. Barbier and Caroline Fontaine randomized the bounded syndrome coding problem on wet paper—an important embedding problem in steganography—such that this problem always has a solution [24]. This randomization is inspired the Courtois–Finiasz–Sendrier signature scheme, and shows nice results for linear perfect codes. In the special case of binary Hamming codes, this new method reaches exactly the necessary and sufficient bounds to ensure the embedding. The previous bounds were introduced by Carlos Munuera and M. Barbier [19]. These bounds depend on the dual distance of the code used. Thanks to the generalized Hamming weight, they proved that codes with low MDS rank are better in this context. Since the nature of their results are combinatorial, the authors generalized a bound for systematic non linear codes and showed that the non-linear systematic codes could be good candidates, as shown by the example of the Nadler code.

6.4. Homomorphic encryption

D. Augot, in collaboration with L. Perret from Salsa team, and Bochum Universität [22], designed a "secret-key" homomorphic encryption scheme, which is much more efficient than the public-key ones. It is based on q-ary Reed-Muller codes (or multi-variate evaluation-interpolation schemes). The main drawback is a severe restriction on the number of uses of a given secret key, but the ease of decrypting leads to think that the scheme can reencrypt its keys, enabling its reuse.

6.5. List decoding

D. Augot, M. Barbier and A. Couvreur wrote on how to decode binary Goppa codes. Augot, Barbier, and Couvreur presented a simple way, with a clean study of the complexity [23]. Using this list decoding algorithm, Barbier and Paulo Barreto proposed a key reduction for the McEliece cryptosystem [25]. The list decoding algorithm above allowed them to add more errors during the McEliece encryption step, making decoding attacks more difficult. At the same complexity of these attacks, using the list decoding algorithm decreases the public key size, which is the main drawback of this cryptosystem.

6.6. Explicit isogeny constructions

B. Smith constructed six infinite series of families of pairs of algebraic curves of arbitrarily high genus [20], defined over number fields, together with an explicit isogeny between the Jacobians of the curves splitting multiplication by 2, 3, or 4.

6.7. Quasi-cyclic codes

M. Barbier, Christophe Chabot and G. Quintin exhibited a bijective correspondence between the ℓ-quasi-cyclic codes over $\mathbb{F}_q$ of length $m\ell$ and the set of ideals of $M_\ell(\mathbb{F}_q)[X]/(X^m-1)$ [29]. They proposed also two new classes called the quasi-BCH and quasi-evaluation codes. For the first one, they introduced a unambiguous decoding algorithm, and thanks to the second one they designed 49 new codes over $\mathbb{F}_4$ which have a bigger minimum distance than previously known codes.

6.8. Root-finding over Galois rings

Jérémy Berthomieu, Grégoire Lecerf and G. Quintin presented a new algorithm to find all the roots of a given polynomial with coefficients in a Galois ring [30]. It has been used to study the behavior of the Sudan algorithm for Reed-Solomon codes over Galois rings. The algorithm has been adapted to work over rings of power series in several variables. It was implemented in the Quintix package of Mathemagix.

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.
- D. Augot, with Christine Eisenbess, 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. Partnerships and Cooperations

8.1. Regional Initiatives

- DIGITEO 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 contributed a postdoctoral salary to the project (see National Initiatives).

8.2. National Initiatives

- The DGA funded a postdoctoral researcher's salary for Sorina Ionica, allowing her to join TANC for one year (10/2010–09/2011) as a postdoctoral researcher for the AMIGA project.
- The team received DGA funding for the project DIFMAT, joint with ENSTA, to find good MDS matrices, which are used for diffusion in block ciphers. The period is October 2011–September 2012, eventually renewable one year.

8.3. European Initiatives

8.3.1. Major European Organizations with which Tanc has followed Collaborations

Partner 1: Ulm Universität, TAIT group, Germany.

Subject 1: bridging Ulm's unique decoding with Guruswami-Sudan list decoding. Funded by a PHC Hubert Curien.

8.4. International Initiatives

8.4.1. INRIA International Partners

- DTU, Denmark.

8.4.2. Visits of International Scientists

- Kamal Khuri–Makdisi, American University of Beirut, two weeks.
- Iwan Duursma, University of Illinois at Urbana Champaign, two weeks,

9. Dissemination

9.1. Animation of the scientific community

- D. Augot is a member of the scientific committee for the French CCA seminar.
- D. Augot was co-chair, with Anne Canteaut, of WCC 2001, and is guest editor of a special issue of Design, Codes, and Cryptography dedicated to the conference.
- F. Morain was invited speaker at the C2 meeting (Ile d'Oléron, spring 2011).
- F. Morain gave two lectures in the summer school linked to ECC2011.
- B. Smith organised the rump session at ECC2011.

9.2. Teaching

D. Augot

18 hours, "Codes correcteurs d'erreurs et applications à la cryptographie", M2, MPRI, France.

F. Morain:

10 lectures of 1.5h, 1st year course "Introduction à l'informatique" (INF311) at École polytechnique.

7.5h Algorithmes arithmétiques pour la cryptologie, M2, MPRI, France.

B. Smith:

INF321: Les principes des langages de programmation, 40h (TD), L1, École polytechnique, France

Algorithmes arithmétiques pour la cryptologie, 9h, M2, MPRI, France

PhD & HdR (Les thèses soutenues doivent figurer dans la bibliographie) :

PhD: Morgan Barbier, "Décodage en liste et application à la sécurité de l'information", defended December 2nd, 2011, D. Augot.

PhD in progress : Cécile GONÇALVES, Advanced cardinality algorithms for cryptographically interesting curves, 01/10/2011, F. Morain and B. Smith

9.3. Popular Science

- D. Augot made a presentation “Quand 1+1=0” to Lycée students at Savigny-sur-Orge.
- D. Augot participated in a S[cube] meeting at Gif-sur-Yvette, about mathematicians.
- D. Augot was interviewed for a video about Évariste Galois.
- D. Augot, M. Barbier, C. Gonçalves, S. Ionica, and B. Smith took part in the “Nuit des chercheurs” at the École polytechnique.

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° 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° 4, p. 505-529.

Publications of the year

Articles in International Peer-Reviewed Journal

[15] A. COUVREUR. *Construction of rational surfaces yielding good codes*, in "Finite Fields and Their Applications", September 2011, vol. 17, n° 5, p. 424-441 [*DOI :* 10.1016/J.FFA.2011.02.007], http://hal.inria.fr/inria-00547454/en.

[16] A. COUVREUR. *Differential Approach for the Study of Duals of Algebraic-Geometric Codes on Surfaces*, in "Journal de Théorie des Nombres de Bordeaux", January 2011, vol. 23, n° 1, p. 95-120, http://hal.inria.fr/inria-00541894/en.

[17] A. COUVREUR. *Incidence structures from the blown-up plane and LDPC codes*, in "IEEE Transactions on Information Theory", July 2011, vol. 57, n° 7, p. 4401 - 4416, Ce travail a été partiellement financé par l'ANR-08-EMER-003, Projet COCQ [*DOI :* 10.1109/TIT.2011.2146490], http://hal.inria.fr/inria-00540023/en.

[18] L. DE FEO. *Fast algorithms for computing isogenies between ordinary elliptic curves in small characteristic*, in "Journal of Number Theory", May 2011, vol. 131, n° 5, p. 873-893 [*DOI :* 10.1016/J.JNT.2010.07.003], http://hal.inria.fr/hal-00505798/en.

[19] C. MUNUERA, M. BARBIER. *Wet paper codes and the dual distance in steganography*, in "Advances in mathematics of communications", November 2011, http://hal.inria.fr/inria-00584877/en.

[20] B. SMITH. *Families of explicitly isogenous Jacobians of variable-separated curves*, in "LMS Journal of Computation and Mathematics", August 2011, vol. 14, p. 179-199 [*DOI :* 10.1112/S1461157010000410], http://hal.inria.fr/inria-00516038/en.

[21] A. ZEH, C. GENTNER, D. AUGOT. *An Interpolation Procedure for List Decoding Reed–Solomon codes Based on Generalized Key Equations*, in "IEEE Transactions on Information Theory", September 2011 [*DOI :* 10.1109/TIT.2011.2162160], http://hal.inria.fr/inria-00633205/en.

International Conferences with Proceedings

[22] F. ARMKNECHT, D. AUGOT, L. PERRET, A.-R. SADEGHI. *On constructing homomorphic encryption schemes from coding theory*, in "IMA International Conference on Cryptography and Coding", Oxford, Royaume-Uni, L. CHEN (editor), Springer, December 2011, http://hal.inria.fr/hal-00643774/en/.

[23] D. AUGOT, M. BARBIER, A. COUVREUR. *List-Decoding of Binary Goppa Codes up to the Binary Johnson Bound*, in "IEEE Information Theory Workshop", Paraty, Brésil, S. AMIN, V. C. DA ROCHA JR., S. I. R. COSTA (editors), IEEE, October 2011, http://hal.inria.fr/hal-00643794/en/.

[24] D. AUGOT, M. BARBIER, C. FONTAINE. *Ensuring message embedding in wet paper steganography*, in "IMACC 2011", Oxford, United Kingdom, L. CHEN (editor), Lecture Notes in Computer Science, November 2011, http://hal.inria.fr/hal-00639551/en.

[25] M. BARBIER, P. S. L. M. BARRETO. *Key Reduction of McEliece's Cryptosystem Using List Decoding*, in "International Symposium of Information Theory (ISIT)", Saint-Peterburg, Russian Federation, A. KULESHOV, V. M. BLINOVSKY, A. EPHREMIDES (editors), IEEE, August 2011, p. 2657-2661, http://hal.inria.fr/inria-00565343/en.

[26] *Best Paper*
P. GAUDRY, D. KOHEL, B. SMITH. *Counting Points on Genus 2 Curves with Real Multiplication*, in "ASIACRYPT 2011", Seoul, Korea, Republic Of, D. H. LEE, X. WANG, H. J. KIM (editors), Lecture Notes in Computer Science, Springer, November 2011, vol. 7073, http://hal.inria.fr/inria-00598029/en.

Scientific Books (or Scientific Book chapters)

[27] A. GUILLEVIC, N. EL MRABET, S. IONICA. *Efficient multiplication in finite field extensions of degree 5*, in "Progress in Cryptology-Africacrypt 2011", Springer, June 2011, n^{o} 6737, p. 188-205, http://hal.inria.fr/inria-00609920/en.

Research Reports

[28] S. IONICA, A. JOUX. *Pairing the Volcano*, October 2011, http://hal.inria.fr/hal-00448031/en.

Other Publications

[29] M. BARBIER, C. CHABOT, G. QUINTIN. *On Quasi-Cyclic Codes as a Generalization of Cyclic Codes*, 2011, under submission, http://hal.inria.fr/inria-00615276/en.

[30] J. BERTHOMIEU, G. LECERF, G. QUINTIN. *Polynomial root finding over local rings and application to error correcting codes*, This work has been partly supported by the French ANR-09-JCJC-0098-01 MaGiX project, and by the Digiteo 2009-36HD grant of the Région Île-de-France., http://hal.inria.fr/hal-00642075/en/.

[31] B. SMITH. *Computing low-degree isogenies in genus 2 with the Dolgachev-Lehavi method*, http://hal.inria.fr/inria-00632118/en.

References in notes

[32] 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.

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

[34] 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.

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

[36] 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.

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

[38] 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.

[39] 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.

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

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] 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.

[46] 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.

[47] 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.

[48] 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.

[49] 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.

[50] 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.

[51] 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.

[52] P. GAUDRY, É. SCHOST. *Genus 2 point counting over prime fields*, 2011, To appear in J. Symb. Comput..

[53] 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.

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

[55] 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.

[56] 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.

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

[58] 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.

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

[60] 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.

[61] 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.

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

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

[64] 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.

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

[66] 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.

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