INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team tanc

Théorie algorithmique des nombres pour la cryptologie

Futurs

THEME SYM

Activity Report

2004

Table of contents

1. Team

Head of project-team

François Morain [Associate professor at École polytechnique]

Vice-head of project team

Pierrick Gaudry [Research scientist]

Staff member INRIA

Andreas Enge [Research scientist]

Doctoral students

Régis Dupont [Corps des Télécom, since 2003-09-01]
Thomas Houtmann [ENS Cachan until 2004-08-31, CNRS/DGA since 2004-09-01]

Administrative Assistants

Catherine Moreau [Administrative Assistant]

External researchers

Nicolas Gürel [defended on 2003-12-15, ATER Marne la vallée]

Post-doctorates

Annegret Weng [august-october 2004]

Student interns

Benoît Libert [Belgian student, co-advisor A. Enge]
Jean-René Reinhard [DEA Algo, april-july 2004]

2. Overall Objectives

TANC is located in the Laboratoire d'Informatique de l'École polytechnique (LIX).

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

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

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

Our research area comprises:

- Fundamental algorithmic arithmetic: we are interested in primality proving algorithms based on elliptic curves (F. Morain being the world leader in this topic), integer factorization, and the computation of discrete logarithms over finite fields. These problems lie at the heart of the security of arithmetic based cryptosystems.
- 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 cryptosystems.
- Algebraic curves over finite fields: the algorithmic problems that we tackle deal with the efficient computation of group laws on Jacobians of curves, evaluation of the cardinality of these objects, and the study of the security of the discrete logarithm problem in such groups. These topics are the crucial points to be solved for potential use in real crypto-products.

3. Scientific Foundations

Keywords: *Cryptology*, *arithmetic*.

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

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

Of course, everything has to be presented in the modern language of complexity theory: computing E and D must be doable in polynomial time; finding D with E alone must be done only in exponential time (say), without some secret knowledge.

Now, where do difficult problems come from? Lattice theory is one point, though the resulting cryptosystems turned out to be too weak. Arithmetic is the next available field of problems. There we find the integer factoring problem, the discrete logarithm problem, etc. All these now form cryptographic primitives that need to be assembled in protocols, and finally in commercial products.

Our activity is concerned with the beginning of this process: we are interested in difficult problems arising in computational number theory and the efficient construction of these primitives.

4. Application Domains

Our main field of applications is clearly that of telecommunications. We participate to the protection of information. We are more on a theoretical level, but also ready to develop applications using modern techniques and objects used in cryptology, with a main focus on elliptic curve cryptography.

5. Software

F. Morain has been improving his primality proving algorithm called ECPP. Binaries for version 6.4.5 are available since 2001 on his web page. Proving the primality of a 512 bit number requires less than a second on a GHz PC. His personal record is about $\approx 10,000$ decimal digits, with the fast version he developped last year.

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

http://www.lix.polytechnique.fr/Labo/Andreas.Enge/Software.html This library is used in our team to build curves with complex multiplication, and is *de facto* incorporated in the ECPP program.

6. New Results

6.1. Complex multiplication

6.1.1. Genus 1

Participants: Régis Dupont, Andreas Enge, François Morain.

Elliptic curves with complex multiplication (e.g., the curve of equation $y^2 = x^3+x$) are the main component of the ECPP algorithm developed by F. Morain, whose aim is to give a primality proof for an arbitrary integer. Though the decision problem ISPRIME? was recently shown to be in *P* (by the work of Agrawal, Kayal, Saxena), practical primality proving is done only with ECPP. This work of AKS has motivated the work of F. Morain on a fast variant of ECPP, called fastECPP, who led him to gain one order of magnitude in the complexity of the problem. The complexity of this variant is heuristically $O((\log N)^{4+\epsilon})$. By comparison, the best proven version of AKS has complexity $O((\log N)^{6+\epsilon})$ and has not been implemented so far (see [13]). F. Morain implemented fastECPP and was able to prove the primality of $10,000$ decimal digit numbers [35], as opposed to $5,000$ for the basic (historical) version. Continuously improving this algorithm, this led to new records in primality proving, some of which obtained with his co-authors J. Franke, T. Kleinjung and T. Wirth [16] who developed their own programs. The current world record was set to 15071 decimal digits early july this year, as opposed to 8000 a year ago.

Curves with complex multiplication are very interesting in cryptography, since computing their cardinality is easy. This is in contrast with random curves, for which this task is still cumbersome. These CM curves enabled A. Enge, R. Dupont and F. Morain to give an algorithm for building good curves that can be used in identity based cryptosystems (cf. infra).

CM curves are defined by algebraic integers, whose minimal polynomial has to be computed exactly, its coefficients being exact integers. The fastest algorithm to perform these computations requires a floating point evaluation of the roots of the polynomial to a high precision. F. Morain on the one hand and A. Enge (together with R. Schertz) on the other, have developed the use of new class invariants that characterize the CM curves. The union of these two families is actually the best that can be done in the field (see [29]). 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 [30]. These invariants, together with this new algorithm, are incorporated in the working version of the program ECPP.

A. Enge has been able to analyse precisely the complexity of class polynomial computations via complex floating point approximations. In fact, this approach has recently been challenged by algorithms using p-adic liftings, that achieve a running time that is (up to logarithmic factors) linear in the output size. He has shown that the algorithm using complex numbers, in its currently implemented form, has a slightly worse asymptotic complexity (polynomial with exponent 1.25). Using techniques from fast symbolic computation, namely multievaluation of polynomials, he has obtained an asymptotically optimal (up to logarithmic factors) algorithm with floating point approximations. The implementation has shown, however, that in the currently practical range, the asymptotically fast algorithm is slower than the previous one. This is due, on the one hand, to the multitude of algorithmic improvements introduced in [29], on the other hand, to the lack of logarithmic factors and better constants. A publication is in preparation.

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

Exploiting the deep connection between the arithmetic-geometric mean (AGM) and a special kind of modular forms known as theta constants, he devised an algorithm based on Newton iterations and the AGM that has quasi-optimal 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 [27].

6.1.2. Genus 2

Participants: Pierrick Gaudry, Thomas Houtmann, Régis Dupont, Annegret Weng.

The theory of Complex Multiplication also exists for non-elliptic curves, but is more intricate. P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler and A. Weng [33] have designed a new approach for constructing class polynomials of genus 2 curves having CM. The main feature of their method is the use of p-adic numbers instead of complex floating point approximations. Although not always applicable, the corresponding algorithm is very efficient compared to previous approaches.

Building upon his work in genus 1, R. Dupont is developping a similar algorithm in genus $g = 2$, aiming at computing class polynomials and modular polynomials, using complex floating point evaluations. His algorithm uses what is known as Borchardt's mean (it can be seen as a generalization of the AGM). A byproduct of that work is an algorithm to compute the Riemann matrix of a given genus 2 curve: given the equation of a such a curve, it computes a lattice L such that the jacobian of the curve is isomorphic to $\mathbb{C}/L$. The algorithms obtained both for the computation of Riemann matrices and for the evaluation of genus 2 modular forms such as the theta constants are quasi-optimal.

6.2. Algebraic curves over finite fields

Participants: Andreas Enge, Pierrick Gaudry, Nicolas Gürel.

In order to build a cryptosystem based on an algebraic curve over a finite field, one needs to efficiently compute the group law (hence have a nice representation of the elements of the Jacobian of the curve). Next, computing the cardinality of the Jacobian is required, so that we can find generators of the group, or check the difficulty of the discrete logarithm in the group.

6.2.1. Effective group laws

A curve that interests us is typically defined over a finite field $\mathrm{GF}(p^n)$ where p is the characteristic of the field. Part of what follows does not depend on this setting, and can be used as is over the rationals, for instance.

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

A. Enge and N. Gürel have been working with J. -C. Faugère and A. Basiri (LIP 6) on the arithmetic of superelliptic and $C_{a,b}$ curves, the next complex class of algebraic curves after the well understood hyperelliptic ones. They have dramatically improved the existing algorithms and have found new algorithms for superelliptic cubic curves, that is, curves of the form $y^3 = f(x)$ with $\deg(f)$ prime to 3 and at least 4[20]. They have generalised their work, in part based on Gröbner basis computations, to $C_{3,4}$ curves and have provided explicit formulae for realising the group law using only operations in the underlying (finite) field [14].

6.2.2. Cardinality

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

Two parameters enter the scene: the genus g of the curve, and the characteristic p of the underlying finite field. When $g = 1$ and p is large, the only current known algorithm for computing the number of points of $E/\mathrm{GF}(p)$ is that of Schoof–Elkies–Atkin. Thanks to the works of the project (actually, *before* joining INRIA), world-widespread implementations are able to build cryptographically strong curves in less than one minute on a standard PC.

When p is small, with one of the most interesting cases for hardware implementation in smart cards being $p = 2$, the best current methods are p-adic methods, 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 using an AGM approach. Developped by R. Harley and P. Gaudry, it led to new world records. Then, P. Gaudry combined this method together with other approaches, to make it competitive for cryptographic sizes [32].

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 [19]. To get one step further, one needs to use genus 2 analogues of modular equations. After a theoretical study [24], 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 are competitive in practice (only three times slower than in the case $g = 1$). In another direction, Kedlaya has introduced a new approach, based on the Monsky-Washnitzer cohomology. His algorithm works originally when $p > 2$. P. Gaudry and N. Gürel implemented this algorithm and extended it to superelliptic curves, which had the effect of adding these curves to the list of those that can be used 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 [31]). 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 [15]. Primes p around 10^9 are now doable.

6.3. Cryptographic protocols

6.3.1. Identity based cryptosystems

Participants: Régis Dupont, Andreas Enge.

Elliptic curves in cryptography have first been used to replace finite fields in protocols whose security relies on the discrete logarithm problem, essentially keeping the protocols as they are and substituting one algebraic structure for another. There are, however, new applications of elliptic curves that exploit specific additional structures that are not found in the finite field setting, for instance the Tate and Weil pairings.

Everybody knows that the most difficult problem in modern cryptography, and more precisely its would-be widespread use, is the key authentification problem, or more generally that of authenticating principals on an open network. The "classical" approach to this problem is that of a *public key infrastructure* (PKI), in which some centralized or decentralized authority issues certificates for authenticating the different users. Another approach, less publicized, is that of *identity based cryptography* (ID), in which the public key of a user can be built very easily from his email address for instance. The cryptographic burden is then put on the shoulders of the *private key generator* (PKG) that must be contacted by the users privately to get his secret key and open their emails. The ID approach can be substituted to the PKI approach in some cases, where some form of ideal trustable PKG exists (private networks, etc.).

This ID idea is not new, but no efficient and robust protocol was known prior to the ideas of Boneh et al. using pairings on elliptic curves. R. Dupont and A. Enge have worked on such an ID-system. They have defined a notion of security for such a protocol and have given a proof of security of a generalization of a system of Sakai, Ohgishi and Kasahara' in this model [28].

6.3.2. CESAM

Participants: Andreas Enge, Pierrick Gaudry.

The CESAM project is a contract of the ACI Sécurité Informatique, involving TANC and the crypto team at ENS. The goal of this project is to study cryptographic protocols involving elliptic curves, with a view towards specific environment where the resources (cpu, memory, bandwidth) are limited.

A first result has been obtained in this framework [26]. An authenticated key exchange algorithm is designed using specific properties of elliptic curves, namely the existence of the *quadratic twist* that we can associate to any elliptic curve. The nice feature of our approach is that it is possible to prove the security of the protocol in the standard model, and in particular without relying on the controversial Random Oracle Model. Indeed, in key exchange protocols, the session key is usually obtained via the application of a hash function to a group element. In our case, this hash function is no longer necessary.

The curves that can be used in this protocol are not the same as the curves that are used in classical protocols, since the group orders of the curve and of the quadratic twist need both to be prime. A. Enge has made use of the complex multiplication approach presented above to generate such curves. Finding curves of cryptographic size (192 bits) is a matter of seconds with his implementation. A note is in preparation.

6.3.3. Security in ad hoc networks

Participant: François Morain.

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

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

6.4. The discrete logarithm in jacobians of curves

Participant: Pierrick Gaudry.

6.4.1. Attacking elliptic curves over small degree extension fields

P. Gaudry [23] has developped an algorithm that can solve the discrete logarithm problem in elliptic curves defined over a finite field of the form $GF(q^n)$, when $n \geq 3$ is a small integer. His algorithm lies in the family of the so-called Weil-descent attacks. The main difference with previously known algorithms is that the use of the theory of function fields is replaced by Gröbner basis computations. As a consequence, the range of application of the algorithm is less restrictive than previously known attacks (that often worked only for small classes of curves). On the other hand, the dependance in n is so bad that only the case $n = 3$ and $n = 4$ are meaningful in practice.

It is important to stress that the two cases widely used in practice, which are $GF(p)$ and $GF(2^n)$ with a prime n, are not vulnerable to this approach. Gaudry's result can be viewed as a confirmation about "bad feelings" that most researcher had about the security of curves over small degree extension fields.

6.4.2. Attacking low genus hyperelliptic curves

P. Gaudry, E. Thomé and N. Thériault [34] have improved index calculus algorithms for computing discrete logarithms in jacobians of hyperelliptic curves of low genus at least 3. Their attack is based on the addition of a double large prime variation to a previously known algorithm. The surprise is that in the case of discrete logarithm of curves, the complexity is improved, whereas in all other application ranges of double large prime variations, the gain is only by a constant factor. Hence, the main difficulty for this work was to provide a complexity analysis that was also validated by numerous computer experiments.

As a consequence, curves of genus 3 and larger than 3 should be used with extreme care when deployed in a cryptosystem. At the very least, a cryptosystem based on a genus 3 curves must have a key-size about 12% larger than an elliptic cryptosystem to offer the same level of security.

7. Contracts and Grants with Industry

- ACI CRYPTO p-ADIQUE: use p-adic numbers un cryptology, especially for computing the cardinality of algebraic curves over finite fields.
- Gemplus : thesis of É. Brier on the use of hyperelliptic curves in cryptology.
- ACI SÉCURITÉ CESAM : elliptic curves for the security of mobile networks.
- ACI SÉCURITÉ SERAC: SEcuRity models and protocols for Ad-hoC Networks.

8. Other Grants and Activities

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

9. Dissemination

9.1. Program committees

A. Enge has been a member of the programme committee of Indocrypt 2004, held in Chennai, India.

9.2. Teaching

François Morain is the head of the 1st year course “Introduction à l’informatique et à la programmation” at École polytechnique, and gives a cryptology course in Majeure 2. He represents École polytechnique in the Commission des Études of the Master MPRI.

A. Enge has been responsible for an introductory course on cryptology for PhD students at the University Bordeaux I. During the summer, he has conceived and realised a multimedia lecture on selected cryptologic topics proposed to students of École polytechnique in the framework of the European project Convergence. Furthermore, he has given lectures on the hyperelliptic discrete logarithm problem during the summer school on elliptic curve cryptography at Bochum.

A. Enge and P. Gaudry give lectures in the MPRI Master. R. Dupont, A .Enge, P. Gaudry, F. Morain, A. Weng have given lectures during the special semester on explicit methods in number theory at Institut Henry Poincaré, Paris (RD on his work, AE/AW/FM on complex multiplication, PG on point counting over finite fields).

P. Gaudry is also active at École polytechnique (Majeure 2, etc.).

F. Morain participated for the second time in the ACM International Programming Contest (SWERC04) in november 2004, as one of the problem authors. This contest was held at École polytechnique.

9.3. Seminars and talks

A. Enge has given a survey on elliptic curve cryptography and recent progress in the field during the “Journée Sécurité de l’Information et Cryptographie” in Limoges in november. He has presented his work on the complexity of class polynomial computation at the workshop “Algorithms and Number Theory” at Dagstuhl in may.

P. Gaudry was a invited speaker for the ECC-2004 conference in Bochum (Germany), 20-22/09/04. He gave a talk during the Journées ACI Sécurité Informatique à Toulouse (16/11/04).

F. Morain has given talks on fastECPP in Amiens, Paris 6, Ensta. He presented [16] in Burlington.

N. Gürel has given talks in Caen; ENSTA; Sydney (Univ. Sydney, Univ. Macquarie) during his postdoctoral stay. R. Dupont has presented his work in Caen (march 2004). T. Houtmann attended Eurocrypt ’04 in Interlaken.

AE, RD, NG, FM all attended ANTS-VI in Burlington.

9.4. Vulgarisation

A. Enge has taken part in the INRIA booth during the “Salon des jeux et de la culture mathématiques” in Paris with a presentation of public key cryptography aimed at a general public. He was an active participant in the “Fête de la Science” at the Ferme du Moulon, proposing activities on secret writing and cryptanalysis to students of age 12 to 14.

10. Bibliography

Major publications by the team in recent years

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

[2] A. ENGE. *Elliptic Curves and Their Applications to Cryptography — An Introduction*, Kluwer Academic Publishers, 1999.

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

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

[5] M. FOUQUET, P. GAUDRY, R. HARLEY. *An extension of Satoh's algorithm and its implementation*, in "J. Ramanujan Math. Soc.", vol. 15, n° 4, 2000, p. 281–318.

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

[7] P. GAUDRY. *Algorithmique des courbes hyperelliptiques et applications à la cryptologie*, Thèse, École polytechnique, December 2000.

[8] P. GAUDRY, R. HARLEY. *Counting points on hyperelliptic curves over finite fields*, in "Algorithmic Number Theory", W. BOSMA (editor)., Lecture Notes in Comput. Sci., 4th International Symposium, ANTS-IV, Leiden, The Netherlands, July 2000, Proceedings, vol. 1838, Springer Verlag, 2000, p. 313–332.

[9] P. GAUDRY, F. HESS, N. SMART. *Constructive and destructive facets of Weil descent on elliptic curves*, in "J. of Cryptology", vol. 15, 2002, p. 19–46.

[10] F. MORAIN. *Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques*, in "J. Théor. Nombres Bordeaux", vol. 7, 1995, p. 255–282.

[11] E. THOMÉ. *Subquadratic computation of vector generating polynomials and improvement of the block Wiedemann algorithm*, in "J. Symbolic Comput.", vol. 33, n° 5, July 2002, p. 757–775.

Articles in referred journals and book chapters

[12] R. DUPONT, A. ENGE, F. MORAIN. *Building curves with small MOV exponent over prime finite fields*, in "J. of Cryptology", to appear, 2004, http://www.springerlink.com/index/10.1007/s00145-004-0219-7.

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

Publications in Conferences and Workshops

[14] A. BASIRI, A. ENGE, J.-C. FAUGÈRE, N. GÜREL. *Implementing the Arithmetic of $C_{3,4}$ Curves*, in "Algorithmic Number Theory — ANTS-VI, Berlin", D. BUELL (editor)., Lecture Notes in Computer Science, vol. 3076, Springer-Verlag, 2004, p. 87–101.

[15] A. BOSTAN, P. GAUDRY, E. SCHOST. *Linear recurrences with polynomial coefficients and computation of the Cartier-Manin operator on hyperelliptic curves*, in "Finite Fields and Applications, 7th International Conference, Fq7", G. MULLEN, A. POLI, H. STICHTENOTH (editors)., Lecture Notes in Comput. Sci., vol. 2948, Springer-Verlag, 2004, p. 40–58.

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

[17] P. GAUDRY. *Chapter 7: Hyperelliptic curves and the HCDLP*, in "Advances in Elliptic Curve Cryptography", I. BLAKE, G. SEROUSSI, N. SMART (editors)., London Mathematical Society Lecture Note Series, In press, Cambridge University Press, 2004.

[18] P. GAUDRY, E. SCHOST. *A low memory parallel version of Matsuo, Chao and Tsujii's algorithm*, in "ANTS-VI", D. BUELL (editor)., Lecture Notes in Comput. Sci., vol. 3076, Springer-Verlag, 2004, p. 208–222.

[19] P. GAUDRY, E. SCHOST. *Construction of Secure Random Curves of Genus 2 over Prime Fields*, in "Advances in Cryptology – EUROCRYPT 2004", C. CACHIN, J. CAMENISCH (editors)., Lecture Notes in Comput. Sci., vol. 3027, Springer-Verlag, 2004, p. 239–256.

Miscellaneous

[20] A. BASIRI, A. ENGE, J.-C. FAUGÈRE, N. GÜREL. *The Arithmetic of Jacobian Groups of Superelliptic Cubics*, To appear in Math. Comp., 2004.

[21] A. ENGE, R. SCHERTZ. *Constructing Elliptic Curves from Modular Curves of Positive Genus*, To appear in Journal de Théorie des Nombres de Bordeaux; available at http://www.lix.polytechnique.fr/Labo/Andreas.Enge/vorabdrucke/cm.ps.gz, 2004.

[22] A. ENGE, R. SCHERTZ. *Modular Curves of Composite Level*, To appear in Acta Arithmetica, available at http://www.lix.polytechnique.fr/Labo/Andreas.Enge/vorabdrucke/modular.ps.gz, 2004.

[23] P. GAUDRY. *Index calculus for abelian varieties and the elliptic curve discrete logarithm problem*, Cryptology ePrint Archive: Report 2004/073, 2004.

[24] P. GAUDRY, É. SCHOST. *Modular equations for hyperelliptic curves*, To appear in Math. Comp., 2004.

[25] F. MORAIN. *Computing the cardinality of CM elliptic curves using torsion points*, Submitted, October 2004.

Bibliography in notes

[26] O. CHEVASSUT, P.-A. FOUQUE, P. GAUDRY, D. POINTCHEVAL. *The 'Twist-AUgmented' approach to authenticated key exchange*, Preprint, 2004, 2004.

[27] R. DUPONT. *Fast evaluation of modular functions using Newton iterations and the AGM*, In preparation, 2004.

[28] R. DUPONT, A. ENGE. *Provably Secure Non-Interactive Key Distribution Based on Pairings*, in "WCC 2003 — Proceedings of the International Workshop on Coding and Cryptography", D. AUGOT, P. CHARPIN, G. KABATIANSKI (editors)., To appear in Discrete Applied Mathematics, École Supérieure et d'Application des Transmissions, 2003, p. 165–174.

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

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

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

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

[33] P. GAUDRY, T. HOUTMANN, D. KOHEL, C. RITZENTHALER, A. WENG. *The p-adic CM-method for genus 2*, In preparation, 2004.

[34] P. GAUDRY, N. THÉRIAULT, E. THOMÉ. *A double large prime variation for small genus hyperelliptic index calculus*, Preprint, 2004.

[35] F. MORAIN. *Implementing the asymptotically fast version of the elliptic curve primality proving algorithm*, In preparation, December 2004.