INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team tanc

Théorie algorithmique des nombres pour la cryptologie

Futurs

THEME 2B

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]
Nicolas Gürel [since 2000-09-01, defense on 2003-12-15]
Thomas Houtmann [ENS Cachan, since 2003-09-01]

Student interns
Ruchir Bindal [IIT New-Delhi, 15-05-2003 to 31-07-2003]

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

Key words: *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 a few seconds on a 700 MHz PC. His personal record is about ≈ 8000 decimal digits, with the fast version he developped this 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

Participants: Andreas Enge, François Morain.

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 $O((\log N)^{4+\epsilon})$. This method has been implemented and was able to prove the primality of 10000 decimal digit numbers [27], as opposed to 5000 for the basic (historical) version. By comparison, the best proven version of AKS has complexity $O((\log N)^{6+\epsilon})$ and has not been implemented so far [17].

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 [5]). 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 [19]. These invariants, together with this new algorithm, are incorporated in the working version of the program ECPP.

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 an active collaboration with J. -C. Faugère and A. Basiri (LIP 6) on the arithmetic of superelliptic cubic curves ($y^3 = f(x)$, with $\deg(f)$ prime to 3 and greater than 3). They have dramatically improved the existing algorithms and have found and implemented new algorithms [29]. Their work, in part based on Gröbner basis computations, generalizes readily to other cubic curves [20].

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 [30].

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 [24].

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 [16]). 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 [21]. Primes p around 10^9 are now doable.

6.3. Identity based cryptosystems

Participants: Régis Dupont, Andreas Enge.

This is a new direction for our project. 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 [18].

6.4. Computing discrete logarithms over finite fields

Participant: Emmanuel Thomé.

E. Thomé has recently devoted most of his time to the finishing of his PhD thesis, defended on May 12, 2003 (he got the Prix de thèse de l'École polytechnique for it). The dissertation's title is "Algorithmes de calcul de logarithme discret dans les corps finis". More precisely, this encompasses a thorough work on the computation of discrete logarithms in finite fields of characteristic 2, which led to a record-size computation of discrete logs in $\mathrm{GF}(2^{607})$. A part of his work has in fact a broader application range, concerning the solving of very large sparse linear systems defined over large prime fields. The algorithm used for solving discrete logarithm problems over $\mathrm{GF}(2^n)$ is a rather standard index-calculus procedure invented by Coppersmith, and augmented with several theoretical and practical improvements that have come over the years. E. Thomé contributed some such improvements. For the linear algebra computation, which is in fact a sub-problem of the discrete logarithm computation, E. Thomé used a "block" version of the Wiedemann iterative method for sparse linear systems. This "block" version is due to Coppersmith. Using the "block" nature of the algorithm, E. Thomé investigated and exploited the possibility of achieving big computations by distributing the work across several machines, and also by taking advantage of the multiprocessor capabilities of the different machines used. Problems previously considered infeasible can now be tackled using "cheap" hardware (in comparison to the hardware typically used for dealing with huge linear systems). The biggest linear algebra problem solved by E. Thomé using this algorithm is a $500,000 \times 500,000$ linear system defined over $\mathrm{GF}(2^{607}-1)$, where the modulus $2^{607}-1$ is here a 182-digit prime.

E. Thomé has also started a cooperation with G. White, a PhD student at the department of mathematics of the university of Sydney, whose aim is to bring to the computer algebra system MAGMA the best of the current technology for computing discrete logarithms in finite fields. In 2001, E. Thomé had already contributed to MAGMA a port of his implementation of Coppersmith's algorithm. E. Thomé and GW started working therefore on the "next step", which is an implementation of the more general *function field sieve* algorithm, which allows computation of discrete logarithms in fields like $\mathrm{GF}(3^n)$ (a strong demand does exist from the cryptologic community to investigate what is in feasible in this area, the interest being spurred in particular by ID-systems based on elliptic curves over $\mathrm{GF}(3^n)$).

Additionally, E. Thomé is currently designing a software library dedicated to computations in p-adic rings and fields. The goal of this library is to achieve high-speed computations on all types of p-adic rings. The speed achieved is evaluated versus handcrafted implementations dedicated to some given problem. While a generic software library cannot be faster than such handcrafted implementations, the objective is to have the library stay on a par with them.

Starting October 1st, 2003, E. Thomé has a permanent research position in the SPACES group at INRIA Lorraine.

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.
- AS of the RTP13 : new trends in cryptography.

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

F. Morain was a member of the program committee of WCC-03, held in Rocquencourt.

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 teaches algorithmic number theory in the DEA-Algo (with G. Hanrot, P. Gaudry).

Andreas Enge participated in the course “Programmation et Algorithmique” of 1st year at École polytechnique.

9.3. Seminars and talks

Andreas Enge was invited to present his work at the school of young researchers in cryptology at Bedlewo, Pologne: "Cryptology - Fundamentals and Frontiers" (05/03).

Pierrick Gaudry presented his work during the Workshop “Next generation cryptography and related mathematics” (Tokyo, Japan, 02/03), in the Workshop “Computational aspects of algebraic curves, and cryptography” (Gainesville, Florida, 03/03), to the Workshop “Cryptography number theory” (London, 04/03), to the conference “Finite Fields and Applications, Fq7” (Toulouse, 05/03), and during the “Rencontres Arithmétiques” (Caen, 06/03). He gave talks at École de cryptologie de Bordeaux (02/03).

François Morain was invited to speak on primality in Lille (31/01/03), to the séminaire Bourbaki (15/03/03). He was invited speaker in Journées du Calcul Formel (Luminy, 01/03). He presented his work with A. Enge on algorithmic Galois theory during the international workshop AAECC-15 (Toulouse, 05/03). He gave a colloquium in Paris 7 (22/05/03) on integer factorization.

10. Bibliography

Major publications by the team in recent years

[1] A. O. L. ATKIN, F. MORAIN. *Elliptic curves and primality proving.* in « Math. Comp. », number 203, volume 61, July, 1993, pages 29–68.

[2] A. ENGE. *Computing Discrete Logarithms in High-Genus Hyperelliptic Jacobians in Provably Subexponential Time.* in « Math. Comp. », number 238, volume 71, 2002, pages 729–742.

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

[4] A. ENGE, P. GAUDRY. *A general framework for subexponential discrete logarithm algorithms.* in « Acta Arith. », number 1, volume CII, 2002, pages 83–103.

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

[6] M. FOUQUET, P. GAUDRY, R. HARLEY. *An extension of Satoh's algorithm and its implementation.* in « J. Ramanujan Math. Soc. », number 4, volume 15, 2000, pages 281–318.

[7] P. GAUDRY, N. GÜREL. *An extension of Kedlaya's point counting algorithm to superelliptic curves.* in « Advances in Cryptology – ASIACRYPT 2001 », series Lecture Notes in Comput. Sci., volume 2248, Springer-Verlag, C. BOYD, editor, pages 480–494, 2001.

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

[9] P. GAUDRY, R. HARLEY. *Counting points on hyperelliptic curves over finite fields.* in « Algorithmic Number Theory », series Lecture Notes in Comput. Sci., volume 1838, Springer Verlag, W. BOSMA, editor, pages 313–332, 2000, 4th International Symposium, ANTS-IV, Leiden, The Netherlands, July 2000, Proceedings.

[10] P. GAUDRY, F. HESS, N. SMART. *Constructive and destructive facets of Weil descent on elliptic curves.* in « J. of Cryptology », volume 15, 2002, pages 19–46.

[11] F. MORAIN. *Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques.* in « J. Théor. Nombres Bordeaux », volume 7, 1995, pages 255–282.

[12] E. THOMÉ. *Subquadratic computation of vector generating polynomials and improvement of the block Wiedemann algorithm.* in « J. Symbolic Comput. », number 5, volume 33, July, 2002, pages 757–775.

Doctoral dissertations and "Habilitation" theses

[13] N. GÜREL. *Conception de cryptosystèmes à base de courbes algébriques.* Thèse, École polytechnique, December, 2003.

[14] E. THOMÉ. *Algorithmes de calcul de logarithme discret dans les corps finis.* Thèse, École polytechnique, May, 2003.

Articles in referred journals and book chapters

[15] R. DUPONT, A. ENGE, F. MORAIN. *Building curves with small MOV exponent over prime finite fields.* in « J. of Cryptology », 2003, http://eprint.iacr.org/2002/094/, to appear.

[16] P. GAUDRY, N. GÜREL. *Counting points in medium characteristic using Kedlaya's algorithm.* in « Experiment. Math. », 2003, http://www.inria.fr/rrrt/rr-4838.html, Version préliminaire comme rapport de recherche INRIA, RR-4838, to appear.

[17] F. MORAIN. *La primalité en temps polynomial (d'après Adleman, Huang ; Agrawal, Kayal, Saxena).* in « Astérisque », 2003, pages Exp. No. 917, Séminaire Bourbaki, Vol. 2002/03, to appear.

Publications in Conferences and Workshops

[18] 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 », École Supérieure et

d'Application des Transmissions, D. AUGOT, P. CHARPIN, G. KABATIANSKI, editors, pages 165–174, 2003.

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

Miscellaneous

[20] A. BASIRI, A. ENGE, J.-C. FAUGÈRE, N. GÜREL. *Implementing the arithmetic of $C_{3,4}$ curves.* 2003, Preprint.

[21] A. BOSTAN, P. GAUDRY, É. SCHOST. *Linear recurrences with polynomial coefficients and computation of the Cartier-Manin operator on hyperelliptic curves.* 2003, To appear in the Proceedings of Finite Fields and Applications, Fq-7.

[22] A. ENGE, R. SCHERTZ. *Constructing elliptic curves from modular curves of positive genus.* 2003, Soumis.

[23] A. ENGE, R. SCHERTZ. *Modular Curves of Composite Level.* 2003, Soumis.

[24] P. GAUDRY, É. SCHOST. *Construction of Secure Random Curves of Genus 2 over Prime Fields.* 2003, Preprint, 14 pages.

[25] P. GAUDRY, É. SCHOST. *Modular equations for hyperelliptic curves.* 2003, To appear in *Math. Comp.*.

[26] F. MORAIN. *Computing the cardinality of CM elliptic curves using torsion points.* October, 2003, Submitted.

[27] F. MORAIN. *Implementing the asymptotically fast version of the elliptic curve primality proving algorithm.* June, 2003, In preparation.

[28] F. MORAIN. *La primalité en temps polynomial.* La Science au présent – Encyclopædia Universalis, 2003, p. 56–57.

Bibliography in notes

[29] A. BASIRI, A. ENGE, J.-C. FAUGÈRE, N. GÜREL. *The Arithmetic of Jacobian Groups of Superelliptic Cubics.* Rapport de Recherche, number RR-4618, INRIA, November, 2002, http://www.inria.fr/rrrt/rr-4618.html.

[30] 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 », series Lecture Notes in Comput. Sci., volume 2501, Springer–Verlag, Y. ZHENG, editor, pages 311–327, 2002.