INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team TANC

Théorie Algorithmique des Nombres pour la Cryptologie

Futurs

THEME SYM

Table of contents

1. Team

Team Leader
François Morain [Associate professor at École polytechnique]

Team Vice-Leader
Pierrick Gaudry [CNRS research scientist, moved to LORIA 2005-09-01]

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 until 2005-01-31, INRIA]
Évelyne Rayssac [Administrative Assistant since 2005-02-01, École polytechnique]

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

Post-doctorates
Javier Herranz [ERCIM, 2005-05-01 until 2006-01-31]
Fabien Laguillaumie [INRIA, 2005-09-01 until 2006-08-31]

Junior technical staff
Jérôme Milan [INRIA, 2005-10-01 until 2006-09-30]

Student intern
Fabien Délen [Université de Versailles-St Quentin, April-July 2005]

2. Overall Objectives

2.1. Main topics

TANC *is located in the Laboratoire d'Informatique de l'École polytechnique (LIX). The project was created on 2003-03-10.*

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

It is clear from this sentence that we combine high-level mathematics and efficient programming. Our main area of competence and interest is that of algebraic curves over finite fields, most notably the computational aspects of these objects, that appear as a substitute of good old-fashioned cryptography based on modular arithmetic. One of the reasons for this change is 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 includes:

- Fundamental number theoretic algorithms: 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.

- Algebraic curves over finite fields: the algorithmic problems that we tackle deal with the efficient computation of group laws on Jacobians of curves, evaluation of the cardinality of these objects, and the study of the security of the discrete logarithm problem in such groups. These topics are the crucial points to be solved for potential use in real crypto-products.
- Complex multiplication: the theory of complex multiplication is a meeting point of algebra, complex analysis and algebraic geometry. Its applications range from primality proving to the efficient construction of elliptic or hyperelliptic cryptosystems.

2.2. Exploratory topics

As described in the name of our project, we aim at providing robust primitives for asymmetric cryptography. In recent years, we have made several attempts at coming closer to another part of cryptology, by applying our knowledge to real life protocols. This has led TANC to recruit two postdocs, one in the framework of ERCIM, and another one from INRIA. The idea was to hire two specialists on signature schemes in which elliptic curves have a decisive impact, since they provide shorter signatures than traditional ones. We are currently trying to promote their use in environments where this could be useful, namely *ad hoc* networks.

In the same vein, we have hired an *ingénieur associé* to write a platform implementing the IEEE P-1363 cryptography standards, so that we can incorporate and test the algorithms normalized in it. This can be used to answer questions on the performance of our systems.

3. Scientific Foundations

3.1. General overview

Keywords: *Cryptology, arithmetic*.

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

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

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

Now, where do difficult problems come from? Mostly from arithmetical problems. There we find the integer factoring problem, the discrete logarithm problem, etc. Varying the groups appears to be important, since this provides some bio-diversity which is the key of the resistance to attacks from crypto-analysts. Among the groups proposed: finite fields, modular integers, algebraic curves, class groups, etc. All these now form cryptographic primitives that need to be assembled in protocols, and finally in commercial products.

Our activity is concerned with the beginning of this process: we are interested in difficult problems arising in computational number theory and the efficient construction of these primitives. TANC concentrates on modular arithmetic, finite fields and algebraic curves.

We have a strong well-known reputation of breaking records whatever the subject is: constructing systems or breaking them, including primality proving, class polynomials, modular equations, computing cardinalities of algebraic curves, discrete logs, etc. This means writing programs and putting in all the work needed to make them run for weeks or months. An important part of our task is now to transform record programs into ones that can solve everyday life problems for current sizes of the parameters.

Efficiency is not our single concern. Certificates are again another one. By this, we mean that we provide proofs of the properties of the objects we build. The traditional example is that of prime numbers, where certificates were introduced by Pratt in 1974. These certificates might be difficult to build, yet they are easy to check (by customers, say). We know how to do this for elliptic curves, with the aim of establishing what we call an **identity card** for a curve, including its cardinality together with the proof of its factorization, its group structure (with proven generators), discriminant (and factorization), class number of the associated order. The theory is ready for this, algorithms not out of reach. This must be extended to other curves, and in several cases, the theory is almost ready or not at all, and algorithms still to be found. This is one of the main problems we have to tackle in TANC.

It is clear that more and more complex mathematics will be used in cryptology (see the recent algorithms that use p-adic approaches). These cannot live if we do not implement them, and this is where we need more and more evolved algorithms, that are for the moment present in very rare mathematical systems, like MAGMA that we use for this. It should be noted that some of our programs (an old version of ECPP, some parts of discrete log computations, cardinality of curves) are now included in this system, as a result of our collaboration with the Sydney group. Once the algorithms work in MAGMA, it is customary to rewrite them in C or C++ to gain speed.

3.2. Algebraic curves over finite fields

One of the most used protocol is that of Diffie-Hellman that enables Alice and Bob to exchange a secret information over an insecure channel. Given a publicly known cyclic group G of generator g, Alice sends g^a for a random a to Bob, and Bob responds with a random g^b. Both Alice and Bob can now compute g^{ab} and this is henceforth their common secret. Of course, this a schematic presentation, since real-life protocols based on this need more security properties. Being unable to recover a from g^a (the discrete log problem – *DLP*) is a major concern for the security of the scheme, and groups for which the *DLP* is difficult must be favored. Therefore, groups are important, and TANC concentrates on algebraic curves, since they offer a very interesting alternative to finite fields, in which the *DLP* can be broken by subexponential algorithms. Thus using curves a smaller key can be used, and this is very interesting as far as limited powered devices are concerned.

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

3.2.1. Effective group laws

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

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

A. Enge and N. Gürel have worked with J. -C. Faugère and A. Basiri (LIP 6) on the arithmetic of superelliptic and $C_{a,b}$ curves, the next complex class of algebraic curves after the well understood hyperelliptic ones. They

have dramatically improved the existing algorithms and have found new algorithms for superelliptic cubic curves, that is, curves of the form $y^3 = f(x)$ with $\deg(f)$ prime to 3 and at least 4[13]. They have generalized their work, in part based on Gröbner basis computations, to $C_{3,4}$ curves and have provided explicit formulae for realizing the group law using only operations in the underlying (finite) field [31].

The great catalog of usable curves is complete, as a result of the work of TANC, notably in two ACI (CRYPTOCOURBES and CRYPTOLOGIE P-ADIQUE) that are finished now.

3.2.2. Cardinality

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

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

When p is small (one of the most interesting cases for hardware implementation in smart cards being $p = 2$) the best current methods use p-adic numbers, following the breakthrough of T. Satoh with a method working for $p \geq 5$. The first version of this algorithm for $p = 2$ was proposed independently by M. Fouquet, P. Gaudry and R. Harley and by B. Skjernaa. J. -F. Mestre has designed the currently fastest algorithm using the arithmetico-geometric mean (AGM) approach. Developed by R. Harley and P. Gaudry, it led to new world records. Then, P. Gaudry combined this method together with other approaches, to make it competitive for cryptographic sizes [40].

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 [10]. To get one step further, one needs to use genus 2 analogues of modular equations. After a theoretical study [18], they are now investigating the practical use of these equations.

When $p = 2$, p-adic algorithms led to striking new results. First, the AGM approach extends to the case $g = 2$ and is competitive in practice (only three times slower than in the case $g = 1$). In another direction, Kedlaya has introduced a new approach, based on the Monsky-Washnitzer cohomology. His algorithm works originally when $p > 2$. P. Gaudry and N. Gürel implemented this algorithm and extended it to superelliptic curves, which had the effect of adding these curves to the list of those usable in cryptography.

Closing the gap between small and large characteristic leads to pushing the p-adic methods as far as possible. In this spirit, P. Gaudry and N. Gürel have adapted Kedlaya's algorithm and exhibited a linear complexity in p, making it possible to reach a characteristic of around 1000 (see [39]). For larger p's, one can use the Cartier-Manin operator. Recently, A. Bostan, P. Gaudry and É. Schost have found a much faster algorithm than currently known ones [33]. Primes p around 10^9 are now doable.

3.3. Complex multiplication

Despite the achievements described above, random curves are sometimes difficult to use, since their cardinality is not easy to compute or useful instances are too rare to occur (curves for pairings for instance). In some cases, curves with special properties can be used. For instance curves with *complex multiplication* (in brief CM), whose cardinalities are easy to compute. For example, the elliptic curve defined over $GF(p)$ of equation $y^2 = x^3 + x$ has cardinality $p + 1 - 2u$, when $p = u^2 + v^2$, and computing u is easy.

The CM theory for genus 1 is well known and dates back to the middle of the nineteenth century (Kronecker, Weber, etc.). Its algorithmic part is also well understood, and recently more work was done, largely by TANC. Twenty years ago, this theory was applied by Atkin to the primality proving of arbitrary integers, yielding the ECPP algorithm developed ever since by F. Morain. Though the decision problem ISPRIME? was shown to be in *P* (by the 2002 work of Agrawal, Kayal, Saxena), practical primality proving is still done only with ECPP.

These CM curves enabled A. Enge, R. Dupont and F. Morain to give an algorithm for building good curves that can be used in identity based cryptosystems (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 CM curves. The union of these two families is currently the best that can be achieved in the field (see [36]). Later, F. Morain and A. Enge have designed a fast method for the computation of the roots of this polynomial over a finite field using Galois theory [37]. These invariants, together with this new algorithm, are incorporated in the working version of the program ECPP.

The theory of Complex Multiplication also exists for non-elliptic curves, but is more intricate, and only recently can we dream to use them. The first results in that direction are described below.

4. Application Domains

4.1. Telecom

Our main field of applications is clearly that of telecommunications. We participate in the protection of information. We are proficient on a theoretical level, as well as ready to develop applications using modern cryptologic techniques, with a main focus on elliptic curve cryptography. One potential application are cryptosystems in environments with limited resources as smart cards, mobile phones or *ad hoc* networks.

5. Software

5.1. ECPP

F. Morain has been continuously improving his primality proving algorithm called ECPP, originally developed in the early '90. Binaries for version 6.4.5 are available since 2001 on his web page. Proving the primality of a 512 bit number requires less than a second on a GHz PC. His personal record is about $\approx 10,000$ decimal digits, with the fast version he started developing in 2003.

5.2. mpc

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

The latest version 0.4.5 has been released in December 2005. This library is used in our team to build curves with complex multiplication, and is *de facto* incorporated in the ECPP program.

We plan to make A. Enge's program that builds elliptic curves with complex multiplication available. This program is a very important building block for cryptographic purposes as well as for primality proving (fastECPP).

6. New Results

6.1. Algebraic curves over finite fields

Participants: Andreas Enge, Pierrick Gaudry, Nicolas Gürel, François Morain.

6.1.1. Effective group laws

P. Gaudry [28] has designed fast formulae for the group law in Jacobians of hyperelliptic curves of genus 2. These formulae are based on the theory of theta functions and work only for base fields of odd characteristic. The number of field operations is significantly less than with previous formulae. A first implementation has been done; on a typical workstation, the running times are essentially the same as for elliptic curves for similar security levels. It is expected that in constrained environments (in particular smart cards), genus 2 cryptosystems that use these formulae should be faster than elliptic curves cryptosystems.

6.1.2. Cardinality

F. Morain, helped by A. Enge and P. Gaudry, has been revisiting the SEA algorithm in genus 1, to see what was left to be improved since the last record, which was achieved in 1995 [43]. This led first to new easy records resulting from Moore's law. The program was completely rewritten of the program was performed in NTL and new algorithms were introduced, concerning mainly the fast search for eigenvalues. The new record is currently (October 2005) for a prime p of 1700 decimal digits (compared to 500dd back in 1995). This was made possible only because of A. Enge new algorithm for computing modular equations of index greater than 2000. These equations are still a stumbling block to reach higher numbers. Several articles are in preparation, describing the improvements to SEA and the computation of modular equations.

We plan to make our new implementation available as an extension to the NTL library.

During his postdoctoral stay in Sydney, N. Gürel worked with D. Kohel and R. Gerkmann on practical aspects of Dwork theory of p-adic differential equations. Based on an unpublished article of N. Tsuzuki, they have constructed the Frobenius matrix of a general family of elliptic curves in characteristic two. In particular, this matrix, whose coefficients are overconvergent series, gives a new point counting method in characteristic two. This work is still in progress.

6.1.3. The discrete logarithm in Jacobians of curves

P. Gaudry [41] 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 applicability of the algorithm is less restrictive than previously known attacks (that often worked only for small classes of curves). On the other hand, the dependence in n is so bad that only the cases $n = 3$ 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 researchers had about the security of curves over small degree extension fields.

P. Gaudry, E. Thomé, N. Thériault and C. Diem [20] have improved index calculus algorithms for computing discrete logarithms in Jacobians of hyperelliptic curves of 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 logarithms 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.

6.2. Complex multiplication

6.2.1. Genus 1

Participants: Régis Dupont, Andreas Enge, François Morain.

The work of AKS motivated the work of F. Morain on a fast variant of ECPP, called fastECPP, which led him to gain one order of magnitude in the complexity of the problem (see [23], [22]), reaching heuristically $O((\log N)^{4+\epsilon})$, compared to $O((\log N)^{5+\epsilon})$ for the basic version. By comparison, the best proven version of AKS has complexity $O((\log N)^{6+\epsilon})$ and has not been implemented so far. F. Morain implemented fastECPP and was able to prove the primality of $10,000$ decimal digit numbers [23], as opposed to $5,000$ for the basic (historical) version. Continuously improving this algorithm, this led to new records in primality proving, some of which obtained with his co-authors J. Franke, T. Kleinjung and T. Wirth [38] who developed their own programs. The current world record was set to 15071 decimal digits early July 2004, as opposed to 8000 a year before.

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

Exploiting the deep connection between the arithmetic-geometric mean (AGM) and a special kind of modular forms known as theta constants, he devised an algorithm based on Newton iterations and the AGM that has quasi-optimal linear complexity. In order to certify the correctness of the result to a specified precision, a fine analysis of the algorithm and its complexity was necessary [14].

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

Using R. Dupont's results described above, A. Enge has devised a second quasi-linear algorithm (that actually even saves a logarithmic factor in the complexity). Breaking the record for class polynomial computations, he has computed a polynomial of degree 100,000, the largest coefficient of which has almost 250,000 bits. For this enormous example, the asymptotically fast algorithm finally beats the one with exponent 1.25. The implementation is based on gmp, mpfr and mpc (see Section 5.2) and a library of A. Enge's for fast arithmetic with polynomials over multiprecision floating point numbers. It turns out that the algorithms are so optimized that the limiting factor becomes the memory consumption [27].

6.2.2. Genus 2

Participants: Pierrick Gaudry, Thomas Houtmann, Régis Dupont.

P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler and A. Weng [29] 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 now developing a similar algorithm in genus 2, aiming at computing class polynomials and modular polynomials using complex floating point evaluations. His algorithm uses what is known as Borchardt's mean (that 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.

R. Dupont has applied his methods to the computation of 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 $p = 2$, and did some partial computations for $p = 3$ (results are available at http://www.lix.polytechnique.fr/Labo/Regis.Dupont).

He also studied more theoretically the main ingredient used in his algorithms in genus 2, a procedure known as Borchardt sequences. In particular, he proved a theorem that parametrizes the set of all possible limits of Borchardt sequences starting with a fixed 4-tuple.

6.3. Cryptographic protocols

6.3.1. Identity based cryptography

Participants: Régis Dupont, Andreas Enge, Javier Herranz.

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 authentication 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 distributed 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 their secret keys 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's in this model [35].

With respect to signatures, a current area of research is related to the aggregation of different signatures on different messages. In many applications, it is desirable to be able to transform many signatures on different messages into a single signature, in such a way that the length of this (aggregate) signature is much less than the total length of the initial signatures. A recipient should be able to verify the correctness of all the initial signatures by using only the list of messages and the aggregate signature, ideally with less computational efforts than in the case where he must verify all the signatures one by one.

For traditional PKI-based signature schemes, some efficient proposals of aggregate signature schemes have been proposed [32], [42]. In particular, in [32], the length of the resulting aggregate signature is constant, independent of the number of messages and the number of signers. This proposal uses bilinear pairings as a tool. Using RSA techniques, the obtained aggregate signatures have a length which is independent of the number of messages, but still linear with respect to the number of signers.

In the scenario of identity-based signatures, none of the existing signature schemes allows an efficient aggregation of signatures, in the sense that resulting aggregate signatures have a length which is always linear with respect to the number of messages. To partially solve this problem, Javier Herranz has proposed in [21] a new identity-based signature scheme, which allows to obtain an aggregate signature whose length is independent of the number of messages, but linear with respect to the number of signers. In situations where one wants to aggregate many signatures coming from a small set of signers (even a unique signer) the length of the resulting signatures is simply constant.

6.3.2. Special (short) signatures

Participant: Fabien Laguillaumie.

To achieve specific properties desired in real-world applications of cryptography, variants of the classical digital signatures have been designed. Undeniable signatures and confirmer signatures are examples of such variants. Directed signatures differ from the well-known confirmer signatures in that the signer has the simultaneous abilities to confirm, deny and individually convert a signature. The universal conversion of these signatures has remained an open problem since their introduction in 1993. F. Laguillaumie, in collaboration with Pascal Paillier (Gemplus) and Damien Vergnaud (Univ. Caen) provides in the Asiacrypt'05 paper "Universally Convertible Directed Signatures" a positive answer to this quest by showing a very efficient design for universally convertible directed signatures, both in terms of computational complexity and signature size. The construction relies on the so-called xyz-trick, previously introduced by F. Laguillaumie and Damien Vergnaud, applicable to bilinear map groups.

F. Laguillaumie, in collaboration with Damien Vergnaud, also introduced a new undeniable signature scheme which is existentially unforgeable and anonymous under chosen message attacks in the standard model [25]. The scheme is an embedding of Boneh and Boyen's recent short signature scheme in a group where the decisional Diffie-Hellman problem is assumed to be difficult. The anonymity of the scheme relies on a decisional variant of the strong Diffie-Hellman assumption, while its unforgeability relies on the strong Diffie-Hellman assumption.

F. Laguillaumie is still working on asymmetric techniques with special properties, concerning both authentication and encryption.

6.3.3. CESAM

Participants: Andreas Enge, Pierrick Gaudry, Nicolas Gürel.

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.

In [34], an authenticated key exchange algorithm is designed using specific properties of elliptic curves, namely the existence of the *quadratic twist* that can be associated to any elliptic curve. The nice feature of this 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 the present 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 both need 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.

In the same direction, N. Gürel [30] has provided new tools to avoid the use of hash functions in elliptic curve key exchange protocols. The method is simple to put in practice, since one just takes some of the bits of the abscissa of a point. The difficult part is to give a rigorous proof that if this point is indistinguishable from a random point then the bits that are extracted are indistinguishable from random bits. N. Gürel proved this result in two contexts: the case where the base field is an extension of degree 2, and in the case where the base field is a prime field. In the former case, one can extract 1/2 of the bits of the abscissa, whereas in the latter case the extraction rate is lower (and depends on the indistinguishability that is required).

6.3.4. Security in ad hoc networks

Participants: François Morain, Javier Herranz, Fabien Laguillaumie.

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

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

A collaboration between TANC (J. Herranz, F. Laguillaumie) and CODES (R. Bhaskar) via the SERAC project of the ACI S&I leads to the submission of "Efficient Authentication for Reactive Routing Protocols" at the SNDS 2006 workshop.

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

Some of these efficiency problems can be reduced with the use of aggregate signatures, which improve the length and the cost of managing many different signatures. In this article, they propose a new concept, aggregate designated verifier signature schemes, which can be implemented in a more efficient way than standard aggregate signatures (for example by using MACs). Such schemes can be sufficient to authenticate the establishment of routes in reactive protocols. Formal definitions for the new primitive and the required security properties are given. Moreover a specific and efficient scheme is proposed which uses MACs, and is proven secure in the random oracle model.

J. Herranz and F. Laguillaumie have started a series of lectures on digital signatures for the members of the SERAC project.

7. Contracts and Grants with Industry

7.1. Gemplus

This corresponds to the thesis of É. Brier on the use of (hyper-)elliptic curves in cryptology.

8. Other Grants and Activities

8.1. Network of excellence

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

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

8.2. ACI

- ACI SÉCURITÉ CESAM: elliptic curves for the security of mobile networks.
- ACI SÉCURITÉ SERAC: SEcuRity models and protocols for Ad-hoC networks.

8.3. Miscellaneous

PAI "Procope" with the group "Algebra and Number Theory" of the TU-Berlin (Florian Heß).

9. Dissemination

9.1. Program committees

F. Morain has been a member of the programme committee of Indocrypt 2005, held in Bangalore, India, in December.

A. Enge has co-organised the Journées Nationales du Calcul Formel 2005 from November 21 to 25 at Luminy.

J. Herranz is in the Program Committee of the conference ACIS'06, to be held in Glasgow next year (May 8-11, 2006).

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 is vice-head of the Département d'Informatique. He represents École polytechnique in the Commission des Études of the Master MPRI.

A. Enge has taught algorithmic number theory and elliptic and hyperelliptic curve cryptography in the MPRI Master. He has given an introductory lecture on hyperelliptic curve cryptology at the École jeunes chercheurs en algorithmique et calcul formel at Montpellier. At École polytechnique, he has proposed computer science labs for the first year course "Introduction à l'informatique" and the second year course "Informatique fondamentale". He has also been responsible for a short course on C programming for third year students.

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).

F. Morain has participated for the third time in the ACM International Programming Contest (SWERC05) in November 2005, as one of the problem authors. This contest was held at École polytechnique.

9.3. Seminars and talks

A. Enge has been an invited speaker at Moraviacrypt '05 — The 5th Central European Conference on Cryptography at Brno, Czech Republic.

He has presented his work at the seminars of the SPACES project at Nancy, of the Algebra and Number Theory group at the TU-Berlin and of the Crypto group at Université Catholique de Louvain. He has spent one week in December with the Algebra and Number Theory group in Berlin.

F. Morain: Barcelona 28-29/10. Winter school CIMPA in Bangalore. SHARCS (Paris, 24-25/02), Eurocrypt'05 (Aarhus, 23-26/05/05); visited University of Calgary ("The end of primality") and workshop in Banff ("SEA++"), November 2005.

N. Gürel has given talks in Limoges (March), Paris 6 (April), ENSTA (October), Rennes (November) and Versailles (December).

Javier Herranz attended Crypto'05 (August 14-18, 2005, Sta. Barbara, California, USA) and the 2nd OLSR Interop & Workshop (July 28-29, 2005, Palaiseau, France, together with F. Morain. A. Enge and T. Houtmann). He spent one week (October 1st-7th, 2005) at Radboud University, invited by the Security of Systems group of that university, in Nijmegen (The Netherlands). There he has given a seminar (October 5th, 2005), entitled 'Aggregate Signatures'.

F. Laguillaumie attended Asiacrypt'05 (December 4–8, Chennai - India) and Indocrypt'05 (December 10–12, Bangalore - India). During Asiacrypt'05, F. Laguillaumie also participates to a meeting between indian and french experts to organize some possible collaborations.

R. Dupont attended “Journées Codage et Cryptographie” (Aussois), Februrary 4, 2005 and presented *Évaluation rapide de formes modulaires via l'AGM*; Number theory seminar, Technische Universität Berlin (Germany), February 9, 2005: *Borchardt's mean, theta constants and applications to the evaluation of Riemann matrices and modular forms*; Séminaire SPACES (LORIA, Nancy), March 3, 2005: *Theta constantes et moyenne de Borchardt, applications*; Séminaire ALGO (INRIA Rocquencourt), November 7, 2005: *AGM, theta constantes et applications*; Journées Nationales de Calcul Formel (CIRM, Luminy), November 25, 2005: *Évaluation rapide de fonctions modulaires via l'AGM*.

T. Houtmann has given talks in Aussois (Journées Codes et Cryptographie 2005), in Caen (April 2005). He attended Eurocrypt'05 in Aarhus, CAEN'05 and XVI-ièmes rencontres arithmétiques de Caen. He attended FICS summer school on elliptic curve cryptography in Copenhagen, ECC2005 in Copenhagen too. He visited the KANT group in Berlin (5-9/12/2005).

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. A. Enge and R. Dupont have presented INRIA at the Forum des métiers scientifiques at École polytechnique. During the welcoming seminar of INRIA, A. Enge has given an overview of the TANC project.

9.5. Editorship

A. Enge is editor of “Designs, Codes and Cryptography”.

9.6. Awards

A. Enge has been awarded a 2004 Kirkman Medal of the Institute for Combinatorics and its Applications. The medal recognises outstanding work by ICA members in their early research careers.

9.7. Thesis committees

F. Morain for M. Finiasz (01/10/04), L. Perret (17/10/05); he wrote reports for that of G. Renault (16/06/05), D. Stehlé (02/12/05); A. Enge for B. Libert.

9.8. Research administration

A. Enge is a member of the International Relations Working Group (GTRI) at the Scientific and Technological Orientation Council (COST) of INRIA. As such, he has participated in two selection rounds of postdoc positions for the European ERCIM consortium and in the selection of international Associated teams.

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, R. SCHERTZ. *Constructing elliptic curves over finite fields using double eta-quotients*, in "Journal de Théorie des Nombres de Bordeaux", vol. 16, 2004, p. 555–568, http://www.lix.polytechnique.fr/Labo/Andreas.Enge/vorabdrucke/cm.ps.gz.

[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] P. GAUDRY, É. SCHOST. *Construction of Secure Random Curves of Genus 2 over Prime Fields*, in "Advances in Cryptology – EUROCRYPT 2004", C. CACHIN, J. CAMENISCH (editors). , Lecture Notes in Comput. Sci., vol. 3027, Springer-Verlag, 2004, p. 239–256, http://www.lix.polytechnique.fr/Labo/Pierrick.Gaudry/publis/secureg2.ps.gz.

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

[12] 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 refereed journals and book chapters

[13] A. BASIRI, A. ENGE, J.-C. FAUGÈRE, N. GÜREL. *The Arithmetic of Jacobian Groups of Superelliptic Cubics*, in "Math. Comp.", vol. 74, 2005, p. 389–410, http://www.inria.fr/rrrt/rr-4618.html.

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

[15] R. DUPONT, A. ENGE, F. MORAIN. *Building curves with arbitrary small MOV degree over finite prime fields*, in "J. of Cryptology", vol. 18, n° 2, 2005, p. 79–89, http://www.lix.polytechnique.fr/Labo/Andreas.Enge/vorabdrucke/mov.ps.gz.

[16] A. ENGE, R. SCHERTZ. *Modular Curves of Composite Level*, in "Acta Arith.", vol. 118, n° 2, 2005, p. 129–141, http://www.lix.polytechnique.fr/Labo/Andreas.Enge/vorabdrucke/modular.ps.gz.

[17] P. GAUDRY. *Advances in Elliptic Curve Cryptography*, I. BLAKE, G. SEROUSSI, N. SMART (editors). , vol. 317, chap. 7: Hyperelliptic curves and the HCDLP, Cambridge University Press, 2005.

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

[19] P. GAUDRY, É. SCHOST, N. M. THIÉRY. *Evaluation properties of symmetric polynomials*, in "Internat. J. Algebra Comput.", To Appear, 2005, http://www.lix.polytechnique.fr/Labo/Pierrick.Gaudry/publis/sym.ps.gz.

[20] P. GAUDRY, E. THOMÉ, N. THÉRIAULT, C. DIEM. *A double large prime variation for small genus hyperelliptic index calculus*, in "Math. Comp.", To Appear, 2005, http://www.loria.fr/~gaudry/publis/dbleLP.ps.gz.

[21] J. HERRANZ. *Deterministic identity-based signatures for partial aggregation*, in "The Computer Journal", to appear, 2005.

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

[23] F. MORAIN. *Implementing the asymptotically fast version of the elliptic curve primality proving algorithm*, in "Math. Comp.", To appear, November 2005, http://www.lix.polytechnique.fr/Labo/Francois.Morain/Articles/fastecpp-final.pdf.

Publications in Conferences and Workshops

[24] F. LAGUILLAUMIE, P. PAILLIER, D. VERGNAUD. *Universally Convertible Directed Signatures*, in "Advances in Cryptology - Proceedings of Asiacrypt'05", B. ROY (editor). , Lecture Notes in Comput. Sci., vol. 3788, Springer-Verlag, 2005, p. 682–701.

[25] F. LAGUILLAUMIE, D. VERGNAUD. *Short Undeniable Signatures Without Random Oracles: the Missing Link*, in "Progress in Cryptology - Proceedings of Indocrypt'05", S. MAITRA, C. E. VENI MADHAVAN, R. VENKATESAN (editors). , Lecture Notes in Comput. Sci., vol. 3797, Springer-Verlag, 2005, p. 283–296.

Miscellaneous

[26] R. BHASKAR, J. HERRANZ, F. LAGUILLAUMIE. *Efficient Authentication for Reactive Routing Protocols*, To appear in Proc. of the Second International Workshop on Security in Networks and Distributed Systems (SNDS-06), 2005.

[27] A. ENGE. *The complexity of class polynomial computation via floating point approximations*, Preprint, 2005, http://www.lix.polytechnique.fr/Labo/Andreas.Enge/vorabdrucke/class.ps.gz.

[28] P. GAUDRY. *Fast genus 2 arithmetic based on Theta functions*, Cryptology ePrint Archive: Report 2005/314, 2005, http://www.lix.polytechnique.fr/Labo/Pierrick.Gaudry/publis/arithKsurf.ps.gz.

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

[30] N. GÜREL. *Extracting bits from coordinates of a point of an elliptic curve*, 2005, http://eprint.iacr.org/.

Bibliography in notes

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

[32] D. BONEH, C. GENTRY, B. LYNN, H. SHACHAM. *Aggregate and verifiably encrypted signatures from bilinear maps*, in "Advances in Cryptology – EUROCRYPT 2003", E. BIHAM (editor). , Lecture Notes in Comput. Sci., vol. 2656, Springer-Verlag, 2003, p. 416–432.

[33] A. BOSTAN, P. GAUDRY, É. SCHOST. *Linear recurrences with polynomial coefficients and computation of the Cartier-Manin operator on hyperelliptic curves*, in "Finite Fields and Applications, 7th International Conference, Fq7", G. MULLEN, A. POLI, H. STICHTENOTH (editors). , Lecture Notes in Comput. Sci., vol. 2948, Springer-Verlag, 2004, p. 40–58, http://www.lix.polytechnique.fr/Labo/Pierrick.Gaudry/publis/cartierFq7.ps.gz.

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

[35] 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.

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

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

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

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

[40] 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.

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

[42] A. LYSYANSKAYA, S. MICALI, L. REYZIN, H. SHACHAM. *Sequential aggregate signatures from trapdoor permutations*, in "Advances in Cryptology – EUROCRYPT 2004", C. CACHIN, J. CAMENISCH (editors). , Lecture Notes in Comput. Sci., vol. 3027, Springer-Verlag, 2004, p. 74–90.

[43] 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.