# Équations modulaires, algorithmes et applications

François Morain, LIX, École Polytechnique

Les équations modulaires ont été introduites il y a fort longtemps, en liaison avec le calcul d'intégrales elliptiques. Au fil du temps, on les as vues comme des modèles des courbes modulaires, typiquement $X_0(N)$. Leur intérêt intrinsèque est grand, comme le démontre le théorème de Wiles. Les courbes modulaires ont permis de construire de bons codes géométriques (Tsfasman, Vladut, Zink; plus récemment les tours de Garcia-Stichtenoth expliquées par Elkies). D'un point de vue plus algorithmique, elles sont la clef de voûte de l'algorithme SEA qui calcule la cardinalité d'une courbe elliptique sur un corps fini. Le but de l'exposé est de présenter quelques éléments de base de la théorie, en insistant sur les calculs de ces équations et les applications aux thèmes déjà cités, en y ajoutant quelques liens avec la théorie de la multiplication complexe.

# Speeding up the CRT method to compute class polynomials in genus 2

Damien Robert, TANC, INRIA Bordeaux Sud-Ouest

Elliptic curve provides efficient and secure public key cryptosystems, and are also used for pairing based cryptography. Using Jacobians of hyperelliptic curve of genus 2 give the same level of security while working on fields of half the size. The theory of Complex Multiplication give an efficient way to construct hyperelliptic curves with a high level security by computing the class polynomials associated to a CM field of degree 4. The CRT method allows to compute these class polynomials in genus 2 for any CM field. However, whereas the record class polynomials computation in genus 1 done by Andrew Sutherland use the CRT approach, in genus 2 the CRT method is slower than the analytic or the $p$-adic lifting method (which only work for more specific CM-fields). In a joint work with Kristin Lauter, we have developed some new tools to speed up the CRT method in genus 2. I will present these ideas, along with some examples from an implementation done in the Magma computer language to show what kind of speed up we obtain in practice.

# Modèle de Kummer en Caractéristique deux

Oumar DIAO

11 février 2011

## Résumé

Dans cet exposé, on s'intéresse au modèle de Kummer défini sur un corps de caractéristique deux en genre plus petit que 2. Soit $C$ une courbe hyperelliptique de genre $g$ et de jacobienne $J_C$, le modèle de Kummer est le quotient de $J_C$ par l'involution hyperelliptique. En caractéristique deux, Gaudry et Lubicz, en 2008, étudient les modèles de Kummer ordinaires en genres 1 et 2 grâce aux fonctions thêta de Rieman. Cependant, leurs formules ne marchent pas pour les modèles de Kummer non-ordinaires.

Pour étudier les modèles non-ordinaires, nous utilisons des techniques de « déformations » qui consistent à considérer une famille de jacobiennes sur un anneau des séries formelles, telle que la fibre générique soit ordinaire et la fibre spéciale soit la jacobienne considérée. Il s'agit alors de montrer que la loi de groupe sur la fibre générique s'étend à tout le modèle. Nous obtenons ainsi des lois de composition très efficaces sur les surfaces de Kummer non-ordinaires par rapport aux formules existantes.

# Isogénies explicites : progrès récents et implantations

Luca De Feo, LIX, École Polytechnique

Une isogénie est un morphisme rationnel de variétés abéliennes qui est aussi un morphisme de groupes. En cryptographie, les isogénies de courbes elliptiques sont utilisées pour le comptage de points, la cryptanalyse, la construction de cryptosystèmes et la détermination de l'anneau d'endomorphismes d'une courbe elliptique.

Par isogénie "explicite" on dénote l'ensemble des problèmes algorithmiques consistant à calculer des expressions rationnelles pour une isogénie donnée (par son noyau, par son image ou par son degré, par exemple). Le calcul d'isogénies explicites a initialement été motivé par l'algorithme de comptage de points SEA, mais vit aujourd'hui sa vie propre grâce aux avancées susmentionnées.

Traditionnellement, le problème de l'isogènie explicite pour les corps fini se décline en deux sous-problèmes qui ont donné vie à des techniques très différentes : le cas de la grande caractéristique (très semblable au cas de la caractéristique 0) et celui de la petite. Ces deux mondes ont récemment été partiellement unifiés par l'algorithme de Lercier et Sirvent.

Dans cet exposé nous allons faire un tour d'horizon des différentes techniques de calcul d'isogénies explicites et nous allons présenter les avancées récentes en matière de complexité et de rapidité des calculs. Nous allons aussi présenter l'état des implantations logicielles en cours.

# Un algorithme à la Pollard pour le problème du sac à dos

Gaëtan Bisson, LORIA, Nancy

Soit $S$ une suite d'éléments d'un groupe fini $G$ noté multiplicativement ; le problème du sac à dos consiste à trouver une sous-suite de $S$ dont le produit vaut un élément donné $z$ de $G$. Des méthodes très efficaces pour le résoudre existent quand $G = \mathbb{Z}/n\mathbb{Z}$ mais elles nous abandonnent lorsque l'on change de groupe : on peut en effet prouver qu'aucun algorithme générique (c'est-à-dire, en un sens, qui s'applique à tout groupe $G$) ne peut résoudre ce problème en moins de $O(\sqrt{\#G})$ opérations.

Si une approche de type "pas de bébé, pas de géant" réussit avec pour complexité $O(\sqrt{\#G})$ en temps et en mémoire, il n'est pas évident de faire mieux. Dans un premier temps, cet exposé aura pour but d'expliquer comment adapter certaines idées de Pollard à ce contexte afin d'obtenir un algorithme en temps $O(\sqrt{\#G})$ et coût mémoire négligeable. Ensuite, nous présenterons certaines applications, notamment à la recherche d'isogénie entre deux courbes elliptiques.

# Vers un nouveau algorithme pour le calcul de l'anneau d'endomorphismes d'une courbe elliptique

Sorina Ionica[1] and Antoine Joux[2]

[1]Laboratoire d'Informatique de l'Ecole Polytechnique (LIX)
[2]DGA and Université de Versailles Saint-Quentin

En 1996, D. Kohel [3] propose un premier algorithme pour le calcul de l'anneau d'endomorphismes d'une courbe elliptique. Sa méthode repose, entre autres, sur un algorithme de parcours en profondeur du graphe d'isogénies (ce qu'on appelle un volcan). Les méthodes existantes à nos jours pour déterminer l'anneau d'endomorphismes [1] utilisent des algorithmes de parcours du graphes d'isogénies. J'expliquerai l'algorithme de D. Kohel et je montrerai, en utilisant de résultats de [2], que l'on peut calculer l'anneau d'endomorphismes sans avoir parcourir les volcans d'isogénies et juste en calculant un petit nombre de couplages. Cela est possible lorsque la factorisation du conducteur de l'anneau d'endomorphismes contient que des facteurs premiers de taille pas très grande. Néanmoins, cette méthode a l'avantage d'éviter des calculs couteaux d'isogénies, en les remplaant par des calculs rapides de couplages.

## Références

1. G. Bisson and A. Sutherland. Computing the endomorphism ring of an ordinary elliptic curve over a finite field. Journal of Number Theory, 2010. to appear.
2. S. Ionica and A. Joux. Pairing the volcano. In Algorithmic Number Theory Symposium, volume 6197 of Lecture Notes in Computer Science, pages 201–218. Springer, 2010.
3. D. Kohel. Endomorphism rings of elliptic curves over finite fields. PhD thesis, University of California, Berkeley, 1996.

# Résolution pratique du problème du logarithme discret dans des courbes elliptiques définies sur des extensions sextiques

V. Vitse, travail commun avec A. Joux

Le *problème du logarithme discret* (DLP) consiste à calculer, étant donnés un groupe fini cyclique $G$ et deux éléments $g, h \in G$, un entier $x$ tel que $h = g^x$. L'ensemble des points rationnels d'une courbe elliptique définie sur un corps fini est naturellement muni d'une loi de groupe dans lequel le DLP s'avère difficile. En effet, on ne connaît en général que des algorithmes exponentiels de complexité asymptotique en $\sqrt{\#G}$ sur $E(\mathbb{F}_q)$, contrairement aux groupes multiplicatifs de $\mathbb{F}_q$ pour lesquels il existe des algorithmes sous-exponentiels. À sécurité comparable, les tailles de clefs utilisées sont donc nettement plus petites que celles que l'on retrouve dans les cryptosystèmes basés sur la factorisation ou sur le DLP dans les corps finis.

Initialement, les premières courbes considérées en cryptographie étaient définies sur un corps fini binaire ou premier. Mais pour accélérer l'arithmétique, d'autres corps de définition ont été proposés. En particulier, les extensions de corps optimales (OEF) sont souvent priviligiées dans les implémentations matérielles : elles sont de la forme $\mathbb{F}_{p^d}$ où $p$ est un nombre de Mersenne pseudo-premier et $d$ est un entier généralement petit pour lequel il existe un polynôme irréductible de la forme $X^d - \omega \in \mathbb{F}_p[X]$. Pourtant, lorsque l'on considère des courbes définies sur des extensions de corps, on peut attaquer le DLP avec des algorithmes spécifiques potentiellement plus performants tels que la descente de Weil ou les méthodes de décomposition dans une base de facteurs. La première méthode consiste à transférer le DLP de $E(\mathbb{F}_{q^n})$ sur la jacobienne d'une courbe $\mathcal{C}$ définie sur $\mathbb{F}_q$ et à utiliser le calcul d'indices sur cette jacobienne pour en déduire le logarithme ; cette approche est efficace lorsque le genre de la courbe $\mathcal{C}$ est petit (idéalement égal à $n$), mais ceci ne se produit que rarement en pratique. L'autre méthode, plus récente, de décomposition s'applique indifféremment à toutes les courbes (hyper-)elliptiques définies sur un corps non premier. Cependant sa complexité, bien qu'asymptotiquement intéressante, n'est en général pas meilleure que celle des attaques génériques pour les tailles de groupes utilisées en pratique.

Dans cet exposé, on présentera une technique combinant les deux approches et qui permet d'attaquer le DLP sur les courbes définies sur des extensions de degré composé. L'idée consiste à d'abord transférer le DLP sur la jacobienne d'une courbe définie sur une extension intermédiaire, puis à utiliser la méthode de décomposition sur cette sous-extension à la place du classique calcul d'indices. En particulier, on donnera un exemple concret d'attaque du DLP pour un sous-groupe de taille 130 bits d'une courbe définie sur $\mathbb{F}_{p^6}$, a priori résistant à toute attaque connue, mais pour lequel notre méthode nous a permis de calculer des logarithmes en environ 3700 h CPU, soit moins de 30h de temps de calcul réel.

# Étude des systèmes polynomiaux intervenant dans le calcul d'indice pour la résolution du problème du logarithme discret sur les courbes

Louise Huot, LIP6, Université Paris 6

Dans la méthode de résolution du DLP sur une courbe elliptique par calcul d'indice (proposée par C. Diem et P. Gaudry indépendemment), une étape cruciale nécessite de décomposer des points sur cette courbe. Une méthode algébrique pour résoudre ce problème est de le modéliser sous forme de systèmes polynomiaux. Pour une courbe elliptique définie par une équation de Weierstrass, Diem et Gaudry modélisent le problème de décomposition d'un point à l'aide des polynômes de Semaev. Dans cet exposé, nous présenterons de nouvelles méthodes pour décrire ce problème sous forme de systèmes polynomiaux à partir de différentes représentations de courbes elliptiques. Nous mettrons en évidence des représentations de courbes telles que les systèmes polynomiaux obtenus ont une structure très particulière. Nous présenterons aussi les résultats pratiques pour la résolution des systèmes générés par chacunes des modélisations et représentations étudiées. Ces travaux permettent d'identifier les représentations qui apportent un gain sur la résolution du problème de décomposition d'un point.

# Univariate Side Channel Attacks and Leakage Modeling

Julien Doget[1,2,3], Emmanuel Prouff[1], Matthieu Rivain[4], and François-Xavier Standaert[2]

[1] Oberthur Technologies,
71-73 rue des Hautes Pâtures, F-92 726 Nanterre, France
{j.doget, e.prouff}@oberthur.com
[2] Université Catholique de Louvain-la-Neuve, UCL Crypto Group,
B-1348 Louvain-la-Neuve, Belgium
fstandae@uclouvain.be
[3] Université Paris 8, Département de Mathématiques,
2, rue de la Liberté, F-93 526 Saint-Denis, France
[4] CryptoExperts,
Paris, France
matthieu.rivain@cryptoexperts.com

**Abstract.** Differential power analysis is a powerful cryptanalytic technique that exploits information leaking from physical implementations of cryptographic algorithms to mount efficient key recovery attacks. During the two last decades numerous variations of the original principle have been published. In particular, the univariate case, where a single instantaneous leakage is exploited, has attracted much research effort. A previous work from Mangard, Oswald and Standaert analysed the asymptotic equivalence of several univariate differential power analysis attacks. It is shown that the statistical tools involved in these attacks only differ in terms that become key-independent once properly estimated. In this talk, we first extend this observation and show that several univariate side channel attacks are not only asymptotically equivalent, but can also be rewritten one in function of the other, only by changing the leakage model used by the adversary. In particular, we show that most univariate differential power analysis attacks proposed in the literature can be expressed as correlation power analyses with different leakage models. This result emphasizes the importance of choosing a good model, namely a model as close as possible to the actual leakage function. As such a model is not always available to the adversary, we also discuss and evaluate side channel attacks that involve no leakage model but rely on some general assumptions about the leakage function. Our experiments show that such attacks, named robust, are a valuable alternative to the univariate differential power analyses. They only loose bit of efficiency in case a perfect model is available to the adversary, and gain a lot in case such information is not available.

# A new Criterion for Effective Algebraic Side Channel Attack

Claude Carlet[1], Jean-Charles Faugère[2], Christopher Goyet[2,3], Guénaël Renault[2]

[1] Université Paris 8, UMR LAGA
INRIA, MTII team
2, rue de la libert
93526 Saint-Denis, Cedex 02, France
[2] UPMC, Université Paris 6, LIP6
INRIA, Centre Paris-Rocquencourt, SALSA Project-team
CNRS, UMR 7606, LIP6
4, place Jussieu
75252 Paris, Cedex 5, France
[3] Thales communications
160 Boulevard de Valmy
92700 Colombes, France
claude.carlet@inria.fr, jean-charles.faugere@inria.fr,
christopher.goyet@fr.thalesgroup.com, guenael.renault@lip6.fr

Algebraic Side Channel Attacks (ASCA) are a new kind of attack recently presented at CHES2009 ([RSVC09]) by Renauld and Standaert. It is a natural combination of classical algebraic cryptanalysis and side channel attacks which take full advantage of both classical attacks. It should be mentioned that several methods combining side channel and algebraic attacks ([BKP08,MME10]) or differential attacks ([HP06,SLFP04]) have already been suggested. Like these papers, the main idea of ASCA is to begin with an on-line phase where leakage information is recorded by a side channel, and to end with a powerful off-line phase where this data is used by algebraic cryptanalysis to recover the key. Contrary to the articles [HP06,SLFP04,BKP08,MME10], ASCA suggests a single-trace scenario. Nevertheless, the side channel information is assumed to be reliable for use in the algebraic attack phase. A CHES2010 paper ([OKPW10]) shows other algebraic approaches for dealing with ASCA in presence of errors. The algebraic attack phase consists of modeling the cryptosystem and the leakage model by a system of polynomial equations, and solving this system to recover the bits of the key.

The main goal of our work is to explain the effectiveness of this attack by describing the criterion of success and therefore to find the theoretical conditions to prevent algebraic side channel attacks. To achieve this goal we assume the same hypothesis as in [RS09,RSVC09], particularly that an initial on-line phases provides a sequence of leakage information, and we only focus on the algebraic cryptanalysis phase. Gröbner techniques are used instead of a SAT-solver. We show that the complexity of the Gröbner basis computation in these attacks depends on a new notion of algebraic immunity and on the distribution of leakage information. This algebraic immunity with leakage is defined by the degree and also the number of lowest degree relations which are given by a black box (SBoxes, Key derivation, etc) and its leakage information. It is an accurate measurement to estimate the complexity of generating a solution. From this new notion of immunity we deduce a criterion for effective Gröbner attacks. For a given block-cipher, this criterion is based on a constant which is easily computed by a local study of the black boxes defining the cryptosystem. A surprising fact is that this criterion also defines a necessary and sufficient condition for SAT-solver attacks. Indeed, this criterion describes several scenarios of unsuccessful Gröbner and SAT-solver attacks. For example if the S-boxes are replaced by functions minimizing the criterion of success then both algebraic attacks become impractical. The same holds when all leakage data minimize the criterion. Thus, this criterion may be seen as an algebraic criterion for effective algebraic side channel attacks.

Our study shows that the AES, SERPENT, PRESENT, CAMELLIA and SMS4 S-boxes are very weak with respect to this criterion. Actually, the local study of these S-boxes shows that the leakage information can be used to partly linearize the system of equations. For example, the probability of obtaining at least 64 (resp. 130) linear relations per round is about 50% for PRESENT (resp. AES).

## References


[BKP08] Andrey Bogdanov, Ilya Kizhvatov, and Andrei Pyshkin. Algebraic methods in side-channel collision attacks and practical collision detection. In *INDOCRYPT*, pages 251–265, 2008.

[HP06] Helena Handschuh and Bart Preneel. Blind differential cryptanalysis for enhanced power attacks. In *Selected Areas in Cryptography*, pages 163–173, 2006.

[MME10] Amir Moradi, Oliver Mischke, and Thomas Eisenbarth. Correlation-Enhanced Power Analysis Collision Attack. In *Workshop on Cryptographic Hardware and Embedded Systems - CHES 2010*. Springer-Verlag, 2010.

[OKPW10] Yossef Oren, Mario Kirschbaum, Thomas Popp, and Avishai Wool. Algebraic Side-Channel Analysis in the Presence of Errors. In *Workshop on Cryptographic Hardware and Embedded Systems - CHES 2010*. Springer-Verlag, 2010.

[RS09] Mathieu Renauld and Francois-Xavier Standaert. Algebraic side-channel attacks. In *Inscrypt 2009*. LNCS, Springer-Verlag, 2009. `http://eprint.iacr.org/2009/279`.

[RSVC09] Mathieu Renauld, François-Xavier Standaert, and Nicolas Veyrat-Charvillon. Algebraic side-channel attacks on the AES: Why time also matters in DPA. In *CHES '09: Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems*, pages 97–111, Berlin, Heidelberg, 2009. Springer-Verlag.

[SLFP04] Kai Schramm, Gregor Leander, Patrick Felke, and Christof Paar. A Collision-Attack on AES Combining Side Channel and Differential Attack. In *Cryptographic Hardware and Embedded Systems - CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings*, pages 163–175. Springer-Verlag, 2004.

# Résistance comparée des automates linéaires à la *SPA*

Laurent Albanese
Nagra France

**Résumé.** Dans cet exposé, nous étudions le comportement d'automates linéaires lorsqu'ils sont soumis à des attaques par canaux cachés de type SPA (*Simple Power Analysis*) en se plaçant dans le cadre du modèle de fuite dit *de la distance de Hamming*. La linéarité des automates nous permet alors de nous ramener dans le cadre du modèle plus simple *du poids de Hamming*. Nous montrons que la plupart des automates ne sont pas sûrs inconditionnellement. Nous caractérisons ensuite deux classes d'automates linéaires. La première présente, vis à vis de la SPA, une résistance inconditionnelle totale. La seconde, plus large, est résistante lorsque le modèle d'observation est affaibli. Les registres à décalage usuels ne font partie d'aucune de ces classes. Nous établissons les équations sous forme algébrique normale des fuites observées lorque les poids de Hamming sont filtrés selon leur décomposition en base 2. Enfin nous fournissons un critère portant sur la matrice de la fonction de transition de l'automate rendant inconditionnellement insoluble le système booléen ainsi filtré.

**Sécurité inconditionnelle des automates linéaires aléatoires.** Soit un automate linéaire :

- dont l'état est un vecteur de $\mathbb{F}_2^n$,
- dont la fonction de transition est représentée par une matrice inversible $A \in GL(n, \mathbb{F}_2)$.

On suppose l'état initial $y$ secret. Seuls sont connus les poids de Hamming des états successifs : $w_0 = w_H(y),\ w_1 = w_H(Ay), \cdots, w_k = w_H(A^k y), \cdots$. Ils constituent les *observations* ; ce sont des entiers compris entre 0 et $n$. Nous montrons alors que *si $A$ est choisie aléatoirement* la connaissance asymptotique de $\frac{2n}{\ln(n)}$ observations suffisent pour déterminer complètement le secret $y$. Ceci sans préjuger d'une méthode effective de résolution.

**Classe inconditionnellement sûre.** Nous montrons que la plus grande résistance aux attaques est atteinte si et seulement si $A$ est une *matrice de permutation*. Dans ce cas, quelque soit le nombre de poids connus, la seule information disponible pour l'adversaire est le poids de Hamming de l'état initial. En contrepartie, les plus grands cycles générés par ces automates ont une taille négligeable devant $2^n$ lorsque $n$ devient grand. En effet, le logarithme de la longueur du plus grand cycle est équivalent à $\sqrt{n \ln(n)}$. Il est toutefois aisé de trouver des états de cycles maximaux.

**Classe résistante au filtrage sur les bits de poids faible du poids de Hamming de l'état interne.** En réduisant les observations modulo 2, on aboutit à un système d'équations linéaires. Pour empêcher la résolution de ce système il faut donc que son rang reste négligeable devant $n$. Le résultat optimal est obtenu lorsque le poids de Hamming des vecteurs colonnes de $A$ est impair. Le système est alors de rang 1. On remarque que les registres à décalage en rebouclage maximal ne vérifient pas ce critère.

**Système filtré sur le $i^{ème}$ bit du poids de Hamming de l'état interne.** En généralisant ce qui précède, il est possible de filtrer le système d'équations en ne considérant qu'un bit d'un rang fixé des poids de Hamming observés (autre que le bit de poids faible). Le système d'équations booléennes obtenues n'est alors plus linéaire. On montre qu'il est de degré $2^{i-1}$ si on filtre sur le $i^{ème}$ bit des observations (en numérotant des bits de poids faibles vers les bits de poids forts).

La matrice $A$ est inconditionnellement résistante vis à vis du $i^{ème}$ bit si :

1. le poids de Hamming des sommes de $k < 2^{i-1}$ vecteurs colonnes est congru à $r < 2^{i-1}$ modulo $2^i$,
2. le poids de Hamming d'une somme de $2^{i-1}$ vecteurs colonnes est congru à $r \geq 2^{i-1}$ modulo $2^i$.

Les matrices respectant ce critère sont celles qui minimisent l'information fournie à l'adversaire.