Courbes elliptiques de Huff et applications cryptographiques

Marc Joye, Techicolor

(Travail commun avec Julien Devigne, Mehdi Tibouchi et Damien Vergnaud)

Dans cet exposé, nous revisitons un modèle pour les courbes elliptiques, introduit par Huff en 1948 dans l'étude d'un problème diophantien. Le modèle de Huff s'applique littéralement aux corps de caractéristique impaire. Toute courbe elliptique sur un tel corps et contenant une copie de $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est birationalement équivalente sur le corps d'origine. Nous étendons et généralisons le modèle de Huff pour couvrir davantage de classes d'isomorphismes de courbes elliptiques. Nous adressons également le cas des corps binaires. Les applications cryptographiques sont discutées. Nous présentons des formules explicites rapides pour l'addition et le doublement de points sur les courbes de Huff généralisées. De façon remarquable, certaines formules obtenues présentent des propriétés intéressantes, y compris le fait d'être complètes et l'indépendance par rapport aux paramètres de la courbe.

CONSTRUCTION OF A k-COMPLETE ADDITION LAW ON ABELIAN SURFACES OVER FINITE FIELDS

CHRISTOPHE ARENE AND ROMAIN COSSET

Nowadays, elliptic curves and more generally abelian varieties are used in cryptography because the discrete logarithm problem is difficult in these groups. To simplify the computation, an easy to compute group law is needed. In this sense, we consider an abelian variety A/k of dimension g embedded in some projective space $\mathbb{P}^r$. Once this embedding is fixed, an addition law is an $(r+1)$-tuple of polynomials that describes the group law on an open subset of the variety.

Definition. A set S of addition laws is said to be *k-complete* if for any point $(x, y) \in (A \times A)(k)$ there is an addition law in S defined on an open subset containing (x, y). S is said to be *complete* if the previous property is true over $\bar{k}$. If $S = \{\mathfrak{p}\}$ is a singleton, we say the addition law $\mathfrak{p}$ is *k-complete* (or *complete* when $k = \bar{k}$).

A k-complete addition law is interesting in practice since it is valid for all couple of points in the group of k-rational points. This is usefull for robustness and is needed for some applications (like for instance on embedded devices).

There exists geometric caracterisations of the possible addition laws. We are particulary interested in addition laws of bidegree $(2, 2)$. This means that the addition law is given by bihomogeneous polynomials in two sets of variables, *i.e.* for each set the polynomials are homogeneous and of degree 2. To ensure the existence of a k-complete addition law, we are led to find a divisor which is symmetric, very ample and k-rational without k-rational points.

In the elliptic curve case, a complete addition law was found by Wieb Bosma and Hendrik W. Lenstra. For A the Jacobian of a genus 2 curve over a finite field classically embedded in $\mathbb{P}^{15}$, the first author with David Kohel and Christophe Ritzenthaler explicit a divisor with the desired properties. To find the k-complete addition law associated to this divisor, we construct a basis of the k-space of addition laws and use an interpolation method to deduce the linear decomposition of the additon law in this basis. The numerical computations are done using AVIsogenies, a Magma package for working with abelian varieties which is developed by Gaetan Bisson, Romain Cosset, and Damien Robert.

Institut de Mathématiques de Luminy, UMR 6206, Luminy, Case 907, 13288 Marseille, France.

E-mail address: arene@iml.univ-mrs.fr

Laboratoire Lorrain de Recherche en Informatique et ses Applications, UMR 7503, Campus scientifique, BP 239, 54506 Vandoeuvre-lès-Nancy, France.

E-mail address: romain.cosset@loria.fr

Algorithmique du décodage en liste de certains codes d'évaluation sur les anneaux finis.

Guillaume Quintin

9 février 2011

Les codes de Reed-Solomon forment une famille de codes à évaluation très utilisée dans l'industrie. Le décodage unique de ces codes est connu et très efficace. Dans [GS98], Guruswami et Sudan ont donné un algorithme de décodage en liste atteignant la borne de Johnson. Dans le même papier il a été généralisé aux codes géométriques. On distingue deux étapes dans cet algorithme : l'étape d'interpollation dans laquelle un polynôme est construit, puis l'étape de recherche de racines qui consiste à trouver les racines du polynôme précédemment construit. Certaines de ces racines sont les mots de codes recherchés et sont donc renvoyés par l'algorithme. Je présenterai l'algorithme bien connu de Guruswami-Sudan, la borne de Johnson et expliquerai le lien entre les deux.

Plusieurs algorithmes pour résoudre les deux étapes ont été proposé pour les codes de Reed-Solomon et géométriques. Dans [Arm05], Marc A. Armand a généralisé la construction des codes de Reed-Solomon pour l'adapter sur des anneaux finis. Les codes de Reed-Solomon sur les anneaux finis ont les mêmes propriétés que leurs homologues sur les corps. Notamment Armand propose un algorithme de décodage en liste atteignant la borne de Johnson. Les codes géométriques peuvent également être généralisé à des codes géométriques sur des anneaux ([Wal99]) et l'algorithme de Guruswami-Sudan adapté ([Bar06]). Je présenterai la construction des codes de Reed-Solomon sur les anneaux et ferai un tour d'horizon des algorithmes existants pour décoder ces codes.

D'autres codes à évaluation ont été étudiés, par exemple les codes à base du théorème des restes Chinois ou *codes CRT*. De même que pour les codes de Reed-Solomon, l'algorithme de Guruswami-Sudan peut être adapté ([Gur05]). Cependant, dans ce cas, la borne de Johnson n'est pas atteinte en temps polynômial. Je montrerai l'algorithme de Guruswami-Sudan pour les codes CRT et expliquerai pourquoi la borne n'est pas atteinte en temps polynômial.

Je conclurai sur les codes à base d'idéaux (d'anneaux) ou *ideal-based codes*. Ces codes ont été introduit par Guruswami-Sudan dans [GSS00]. Ils ont été étudiés un peu plus en détail dans [Gur05]. Guruwsami [Gur03] et Lenstra [Len86] ont proposé la construction de certains de ces codes utilisant des corps de nombres. Mais aucun algorithme de décodage existe à ce jour.

Références

[Arm05] M. A. Armand. List decoding of generalized Reed-Solomon codes over commutative rings. *Information Theory, IEEE Transactions on*, 51(1) :411–419, 2005.

[Bar06] K. G. Bartley. *Decoding algorithms for algebraic geometric codes over rings.* PhD thesis, University of Nebraska, 2006.

[GS98] V. Guruswami and M. Sudan. Improved Decoding of Reed-Solomon and Algebraic-Geometric Codes. *IEEE Transactions on Information Theory*, 45 :1757–1767, 1998.

[GSS00] V. Guruswami, A. Sahai, and M. Sudan. ldquo ;soft-decision rdquo ; decoding of chinese remainder codes. In *Foundations of Computer Science, 2000. Proceedings. 41st Annual Symposium on*, pages 159 – 168, 2000.

[Gur03] V. Guruswami. Constructions of codes from number fields. *IEEE Transactions on Information Theory*, 49(3) :594–603, March 2003.

[Gur05] V. Guruswami. *List Decoding of Error-Correcting Codes : Winning Thesis of the 2002 ACM Doctoral Dissertation Competition (Lecture Notes in Computer Science)*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2005.

[Len86] H. W. Lenstra. *Codes from algebraic number fields*, volume 4, pages 95–104. North-Holland, Amsterdam, 1986.

[Wal99] J. L. Walker. Algebraic geometric codes over rings. *Journal of Pure and Applied Algebra*, 144(1) :91–110, 1999.

Décodage en liste des codes de Goppa Binaire et réduction de clé de McEliece

Morgan Barbier
Laboratoire d'Informatique de l'École Polytechnique - LIX
INRIA Saclay - Île de France
morgan.barbier@lix.polytechnique.fr

Résumé

Le premier décodage algébrique pour les codes de Goppa est dû à Patterson en 1975 [5]. Cette méthode décode jusqu'à t, la capacité de correction du code. Les codes de Goppa font partie de la famille des codes alternants, c'est-à-dire des codes restreints à un sous-corps de Reed-Solomon généralisé, il est donc possible d'adapter toutes les méthodes de décodages des codes de Reed-Solomon aux codes de Goppa, comme le célèbre algorithme de décodage en liste de Guruswami et Sudan [4]. Ce procédé nous permet alors de décoder jusqu'à la borne de Johnson générique, qui est plus grand que t, voire la figure 1. Dans son mémoire de thèse [3], Guruswami propose une méthode pour décoder en liste les codes restreints géométriques jusqu'à la borne de Johnson q-aire, qui est plus grande que la borne de Johnson générique. On propose alors d'appliquer cette même méthode aux codes alternants, et tout particulièrement aux codes de Goppa binaires [1]. Bernstein, Lange et Peters expliquent comment dans le cryptosystème de McEliece, on peut utiliser le décodage en liste [2]. On conclura alors par la réduction de clé de McEliece obtenue grâce à cet algorithme de décodage en liste.

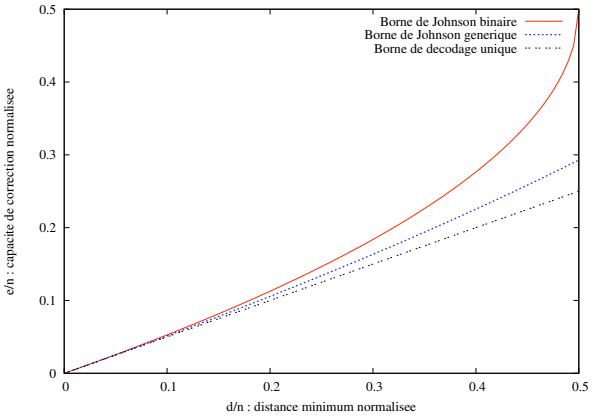

FIGURE 1 – Comparaison de la borne de décodage unique, de Johnson générique et binaire.

Références

[1] D. Augot, M. Barbier, and A. Couvreur, "List-decoding of binary Goppa codes up to the binary Johnson bound," TANC - INRIA Saclay - Polytechnique - Institut de Mathématiques de Bordeaux - IMB, Tech. Rep., 2010. [Online]. Available : http ://hal.archives-ouvertes.fr/inria-00547106/en/

[2] D. Bernstein, T. Lange, and C. Peters, "Attacking and defending the McEliece cryptosystem," in *Post-Quantum Cryptography*, ser. Lecture Notes in Computer Science, J. Buchmann and J. Ding, Eds. Springer Berlin / Heidelberg, 2008, vol. 5299, pp. 31–46.

[3] V. Guruswami, *List Decoding of Error-Correcting Codes - Winning Thesis of the 2002 ACM Doctoral Dissertation Competition*, ser. Lectures Notes in Computer Science. Springer, 2004, vol. 3282.

[4] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon and algebraic-geometry codes," *Information Theory, IEEE Transactions on*, vol. 45, no. 6, pp. 1757–1767, 1999.

[5] N. Patterson, "The algebraic decoding of Goppa codes," *Information Theory, IEEE Transactions on*, vol. 21, no. 2, pp. 203 – 207, Mar. 1975.

A Distinguisher for High Rate McEliece Cryptosystem – Extended Abstract –

Jean-Charles Faugère[1], Ayoub Otmani[2,3], Ludovic Perret[1], and Jean-Pierre Tillich[2]

[1] SALSA Project - INRIA (Centre Paris-Rocquencourt)
UPMC, Univ Paris 06 - CNRS, UMR 7606, LIP6
104, avenue du Président Kennedy 75016 Paris, France
jean-charles.faugere@inria.fr, ludovic.perret@lip6.fr
[2] SECRET Project - INRIA Rocquencourt
Domaine de Voluceau, B.P. 105 78153 Le Chesnay Cedex - France
ayoub.otmani@inria.fr, jean-pierre.tillich@inria.fr
[3] GREYC - Université de Caen - Ensicaen
Boulevard Maréchal Juin, 14050 Caen Cedex, France.

Abstract. The purpose of this talk is to study the difficulty of the Goppa Code Distinguishing (GD) problem, which is the problem of distinguishing the public matrix in the McEliece cryptosystem from a random matrix. It is widely believed that this problem is computationally hard as proved by the increasing number of papers using this hardness assumption. One can consider that disproving/mitigating this hardness assumption is a breakthrough in code-based cryptography. In this paper, we present an efficient distinguisher for alternant and Goppa codes over binary/non binary fields. Our distinguisher is based on a recent algebraic attack against compact variants McEliece which reduces the key-recovery to the problem of solving an algebraic system of equations. We exploit a defect of rank in the (linear) system obtained by linearizing this algebraic system. It turns out that our distinguisher is also highly discriminant. Indeed, we are able to precisely quantify the defect of rank for "generic" binary and non-binary random, alternant and Goppa codes. We have verified these formulas with practical experiments, and a theoretical explanation for such defect of rank is also provided. To our knowledge, this is the first serious cryptographic weakness observed on McEliece since thirty years.

Systèmes Bilinéaires et Déterminantiels : Algorithmes, Complexité et Applications à la Cryptologie.

Pierre-Jean Spaenlehauer
Travail commun avec Jean-Charles Faugère et Mohab Safey El Din

UPMC, Univ Paris 06, LIP6
INRIA, Paris-Rocquencourt Center, SALSA Project
CNRS, UMR 7606, LIP6
Pierre-Jean.Spaenlehauer@lip6.fr

Dans cet exposé, nous nous intéressons à un problème fondamental d'algèbre linéaire : le problème *MinRank*. Étant donnés un corps $\mathbb{K}$, un entier r et une matrice linéaire M de taille $m \times n$ (avec $m \leq n$) sur $\mathbb{K}[x_1, \ldots, x_k]$ (i.e. une matrice dont les entrées sont des formes linéaires en k variables), l'objectif est de trouver l'ensemble des points tels que l'évaluation de M est de rang inférieur ou égal à r. Ce problème est prouvé NP-dur quand $\mathbb{K}$ est un corps fini et il est relié à des applications dans des domaines variés : en cryptologie (cryptanalyse de HFE, authentification zero-knowledge), en théorie des codes (décodage en métrique rang), en géométrie (calcul de points critiques de projections), ...

Nous nous concentrons sur deux modélisations du problème MinRank par des systèmes algébriques multivariés. La première modélisation, proposée par Kipnis et Shamir dans le cadre de la cryptanalyse du système HFE, fait apparaître un système *bilinéaire* en introduisant $n-r$ vecteurs indépendants du noyau de M dont les coefficients sont des indéterminées. La seconde modélisation est donnée par le système constitué de l'ensemble des mineurs de taille $r+1$ de la matrice M (ces mineurs s'annulent sur les solutions du problème MinRank).

Ces systèmes sont ensuite résolus à l'aide d'algorithmes efficaces de calcul de bases de Gröbner. Notre objectif est d'étudier et d'exploiter les propriétés algébriques de ces modélisations pour en améliorer la résolution. Ceci passe par l'obtention de bornes fines sur la régularité et le degré des idéaux étudiés.

Pour étudier la modélisation de Kipnis-Shamir, nous avons besoin de nouveaux résultats théoriques et pratiques sur la résolution des systèmes bilinéaires. En particulier, nous prouvons que le degré de régularité d'un système de $n_x + n_y$ équations bilinéaires affines génériques sur $\mathbb{K}[x_1, \ldots, x_{n_x}, y_1, \ldots, y_{n_y}]$ est borné par

$$\mathsf{d}_{\mathsf{reg}} \leq \min(n_x, n_y) + 1$$

Une conséquence directe de ce résultat est une nouvelle borne sur la complexité de résolution des systèmes bilinéaires affines par des algorithmes de calcul de bases de Gröbner. En praticulier, Faugère, Otmani, Perret et Tilich ont montré que ces résultats permettent d'obtenir des bornes sur la complexité d'attaques algébriques sur certaines variantes compactes de MacEliece.

Du point de vue de la modélisation déterminantielle (i.e. le système constitué des mineurs de taille $r+1$ de la matrice M), nous donnons une forme explicite et *exacte* du nombre de solutions d'un problème MinRank générique :

$$\prod_{i=0}^{m-r-1} \frac{i!(n+i)!}{(m-1-i)!(n-r+i)!}.$$

Nous prouvons également une forme explicite du degré de régularité de l'idéal associé.

Ces formules permettent d'obtenir des estimations précises de complexité asymptotique. En particulier, quand $n = m$ et $k = (n-r)^2$, on montre que le problème MinRank générique peut être résolu en temps polynomial en n : la complexité est alors bornée par $O(n^{3k+1})$. Cette analyse va nous guider vers une estimation précise et effective de la complexité d'un challenge pour un schéma d'authentification de Courtois basé sur le problème MinRank pour lequel aucune attaque praticable n'était connue jusqu'à présent.

Fonctions courbes et "hyper-courbes" en codes et en cryptographie et liens avec les sommes de Kloosterman et les polynômes de Dickson

Sihem Mesnager, LAGA, Université Paris 8 – Université Paris 13

Bent functions are maximally nonlinear Boolean functions with an even number of variables. They were introduced by Rothaus in 1976. For their own sake as interesting combinatorial objects, but also because of their relations to coding theory (Reed-Muller codes) and applications in cryptography (design of stream ciphers), they have attracted a lot of research, specially in the last 15 years. The class of bent functions contains a subclass of functions, introduced by Youssef and Gong in 2001, the so-called hyper-bent functions whose properties are still stronger and whose elements are still rarer than bent functions. Bent and hyper-bent functions are not classified. A complete classification of these functions is elusive and looks hopeless. So, it is important to design constructions in order to know as many of (hyper)-bent functions as possible. This talk is devoted to the constructions of bent and hyper-bent Boolean functions in polynomial forms. We survey and present an overview of the constructions discovered recently. We extensively investigate the link between the bentness property of such functions and some exponential sums (Kloosterman smus and cubic sums) involving Dickson polynomials.

JOURNÉES C2 2011

PROPOSITION D'EXPOSÉ COURT

"VALUATIONS DES SOMMES EXPONENTIELLES"

RÉGIS BLACHE.

L'estimation des valuations p-adiques de sommes d'exponentielles sur un corps de caractéristique p trouve son origine dans l'estimation du nombre de points des variétés algébriques (théorème de Chevalley-Warning). Depuis les travaux de Dwork, elle est liée à l'estimation des valuations des pôles et racines réciproques des fonctions zêta ou L.

Outre son intérêt théorique, elle a des conséquences en théorie de l'information: en particulier sur l'estimation des poids de certains codes ou sur les coefficients de Fourier des fonctions booléennes.

Plus précisément, soit $f \in \mathbf{F}_q[x_1, \cdots, x_n]$ un polynôme, et ψ un caractère additif de $\mathbf{F}_q$; pour chaque entier $m \geq 1$, on définit la somme

$$S_m(f) := \sum_{\mathbf{x} \in \mathbf{F}_{q^m}^r} \psi\left(\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(f(\mathbf{x}))\right),$$

et on associe au polynôme f la fonction L

$$L(f,T) := \exp\left(S_m(f)\frac{T^m}{m}\right),$$

qui est une fraction rationnelle.

Le but est de donner une minoration de la valuation p-adique des sommes $S_m(f)$ quand m varie, ou de façon équivalente, de la valuation p-adique des racines et pôles de la fonction L, c'est à dire d'estimer le polygone de Newton de cette fonction.

Les premiers résultats sont uniformes (en ce sens qu'ils dépendent seulement du degré du polynôme f, ou d'autres invariants associés à ce polynôme); depuis une vingtaine d'années, on a un second type de résultats, qui dépendent aussi de la caractéristique, ou même du cardinal du corps.

En général, les estimations uniformes sont fines quand la caractéristique est grande devant le degré; le besoin de travailler en petite caractéristique (en particulier 2) dicte la recherche d'estimations du second type, et c'est ce sujet qui retiendra notre attention.

On présentera un résumé des développements récents de ce sujet, à travers les travaux de Moreno et ses co-auteurs, et de l'auteur. On exposera en particulier l'évolution d'invariants (p-poids, p-densité) qui permettent de donner des minorations de plus en plus fines.

On donnera aussi des exemples de calculs explicites de la valuation, et certains cas simples où on sait "lire" la valuation de la somme associée à certains polynômes à partir des degrés des monômes qui apparaissent effectivement.

Hachage en temps constant vers les courbes elliptiques

Mehdi Tibouchi, ENS Paris

Dans un certain nombre de protocoles cryptographiques, il est nécessaire de disposer de fonctions de hachage à valeurs dans le groupe des points d'une courbe elliptique. Or construire de telles fonctions de hachage est un problème étonnamment délicat : jusqu'à il y a peu, les solutions connues présentaient pour certaines des problèmes de sécurité et d'efficacité, ou avaient pour d'autres un champ d'application restreint.

On connaît désormais des méthodes satisfaisantes pour ce faire (fournissant une solution en un certain sens idéale). Elles sont obtenues de façon plus géométrique que les techniques antérieures, et leurs propriétés sont établies à l'aide d'outils mathématiques variés. Nous nous proposons de décrire quelques unes de ces méthodes, et d'expliquer comment résoudre certaines des questions qu'elles soulèvent.

The Geometry of Flex Tangents to a Cubic Curve and its Parameterizations*

Jean-Marc Couveignes† and Jean-Gabriel Kammerer‡§

February 11, 2011

Much attention has been focused recently on the problem of computing points on a given elliptic curve over a finite field in deterministic polynomial time. This problem arises in a very natural manner in many cryptographic protocols when one wants to encode messages into the group of points of an elliptic curve. A good example of the algorithmic and cryptologic motivations in finding these parameterizations can be found in the identity-based encryption from [Bo]. The difficulty is to deterministically find a field element x such that some polynomial in x is a square, see [Ko], Section 6.1.8. For example, when the curve is given by a reduced Weierstrass equation $y^2 = x^3 + ax + b$, we deterministically search x such that $x^3 + ax + b$ is a square in the field.

In 2006, Shallue and Woestjine [Sh-Wo] proposed a first practical deterministic algorithm. In 2009, Icart [Ic] proposed another deterministic encoding for elliptic curves over a field with q elements, when q is congruent to 2 modulo 3. Icart's algorithm has quasi-quadratic complexity in $\log q$. Kammerer, Lercier and Renault [Ka-Le-Re] proposed a different parameterization under the additional condition that the elliptic curve has a rational point of order 3, and even for a special class of hyperelliptic curves. Farashahi [Fa] found yet another parameterization for such elliptic curves too. The point is that the map $x \mapsto x^3$ is bijective for finite fields with cardinality congruent to 2 modulo 3. So one looks for a parameterization of the cubic by cubic radicals. This is a special case of the problem of finding parameterizations of curves by radicals [Se-Se, Se-Wi-Pr].

It turns out that such parameterizations closely relate to the geometry of the dual curve of the elliptic curve E. In a nutshell, the dual $\hat{C}$ of a curve C parameterizes the tangents to C. The tangents at the flex points of C correspond to singular points on $\hat{C}$, namely cusps. From rational curves $\hat{R}$ going through these cusps, we can derive pseudo-parameterizations of C. Indeed, to each point on $\hat{R}$ there corresponds a line L in the projective plane. A parameterization of $\hat{R}$ thus gives a family of lines. When the intersection degree of $\hat{R}$ with $\hat{E}$ is even, the intersection of E with L is defined by the roots of a degree 3 polynomial whose discriminant is a square. Then, this discriminant admits a rational root, which gives a point on E.

Such rational curves R can be constructed using the very special configuration formed by the 9 cusps of $\hat{C}$, which correspond to the nine flexes of C.

In this presentation we will review the geometry of the nine flex tangents to a smooth plane cubic C, and we explain how this geometry relates to the parameterizations found by Icart, Farashahi, and Kammerer, Lercier, Renault.

*Research supported by the "Agence Nationale de la Recherche" through project ALGOL (ANR-07-BLAN-0248) and by the French "Délégation Générale pour l'Armement".

†INRIA Bordeaux Sud-Ouest, Université de Toulouse, Institut de Mathématiques de Bordeaux, CNRS.

‡DGA/MI, BP 7 35998 RENNES ARMEES.

§IRMAR, Université de Rennes 1, Campus de Beaulieu, F-35042 Rennes.

The Maple [Wa] code for the calculations in this article can be found on the authors' web pages.

References

[Bo] D. Boneh and M. K. Franklin. Identity-Based Encryption from the Weil Pairing. *CRYPTO*, 2001.

[Fa] R. R. Farashahi. Hashing into Hessian Curves. *Cryptology ePrint Archive, Report 2010/373*, 2010.

[Ic] T. Icart. How to hash into elliptic curves. Proceedings of CRYPTO 2009, pages 303–316. *Lecure Notes in Computer Science, volume 5677. Springer*, 2009.

[Ka-Le-Re] J.-G. Kammerer, R. Lercier, and G. Renault. Encoding points on hyperelliptic curves over finite fields in deterministic polynomial time. International Conference on Pairing-Based Cryptography, 2010.

[Ko] N. Koblitz. Algebraic Aspects of Cryptography. Springer, 1999.

[Sh-Wo] A. Shallue and C. van de Woestijne. Construction of Rational Points on Elliptic Curves over Finite Fields. In Florian Hess, Sebastian Pauli, and Michael E. Pohst, editors, ANTS, pages 510-524. *Lecure Notes in Computer Science, volume 4076. Springer*, 2006.

[Se-Wi-Pr] J. R. Sendra, F. Winkler, and S. Prez-Diaz. Rational Algebraic Curves: A Computer Algebra Approach. *Springer*, 2007.

[Se-Se] R. Sendra and J. Sevilla. Radical Parametrization of Algebraic Curves by Adjoint Curves. ArXiv e-prints 0805.3214, 2008.

[Wa] Waterloo Maple Incorporated. Maple. Waterloo, Ontario, Canada. http://www.maplesoft.com/