Encodage efficace sur différents modèles de courbes elliptiques

T. Alasha (alasha@iml.univ-mrs.fr)
IML, Aix-Marseille Université, France

P. Véron (veron@univ-tln.fr)
IMath/IML, Université du Sud Toulon-Var, France

S. Vlăduţ (vladut@iml.univ-mrs.fr)
IML, Aix-Marseille Université, France

Suite aux progrès dans le domaine de la factorisation [1], l'utilisation des courbes elliptiques en cryptographie à clé publique devrait se généraliser dans les années à venir. En cryptographie elliptique, certains protocoles nécessitent d'être en mesure de pouvoir transformer un élément quelconque de $\mathbb{F}_q$ en un point P de la courbe $E(\mathbb{F}_q)$. Cette opération doit pouvoir être calculée en temps polynomial et de plus, afin déviter les attaques par canaux auxiliaires, elle doit s'effectuer en un nombre constant d'opérations sur le corps $\mathbb{F}_q$. Pour $q \equiv 2 \pmod 3$, l'algorithme le plus efficace pour les courbes définies par l'équation de Weierstrass est celui développé par T. Icart en 2009 [2].

Il existe différentes formes d'équations de courbes elliptiques, la plus répandue et la plus utilisée actuellement correspond au modèle donné par Weierstrass. Cependant des études récentes ont démontré que d'autres modèles (Edwards, Huff, Jacobi) peuvent s'avérer être plus adaptés à certaines problématiques en cryptographie (calcul efficace de pairing, résistance naturelle des formules d'addition aux attaques par canaux auxiliaires). Pour encoder un élément de $\mathbb{F}_q$ sur ces différents types de courbes, on peut utiliser des transformations efficaces permettant de se ramener à l'équation de Weierstrass et appliquer ensuite l'encodage d'Icart [6],[3],[4],[5].

Dans cet exposé, nous proposons pour différents modèles de courbes de nouveaux algorithmes permettant, en un nombre constant d'opérations sur le corps $\mathbb{F}_q$, d'encoder un élément sans avoir à se ramener au modèle de Weierstrass. D'un point de vue applicatif, les algorithmes proposés permettent ainsi de gagner un calcul d'inversion par rapport à la méthode combinant l'encodage d'Icart et la transformation vers le modèle de Weierstrass. De plus, ceci répond à un problème posé par R. Schoof au sujet de l'existence d'un algorithme déterministe permettant de calculer les points rationnels d'une courbe elliptique quelconque [7].

Bibliographie

1. Kleinjung, T., Aoki, K., Franke, J., Lenstra, A.K., Thomé, E., Bos, J.W., Gaudry, P., Kruppa, A., Montgomery, P.L., Osvik, D.A., te Riele, H., Timofeev, A., Zimmermann, P., Factorization of a 768-bit rsa modulus., *Technical report, EPFL IC LACAL and NTT and University of Bonn and INRIA CNRS LORIA and Microsoft Research and CWI (2010)* ,
2. T. Icart, How to Hash into Elliptic Curves, *CRYPTO 2009, LNCS 5677, pp. 303–316, 2009*,
3. R. Feng, and H. Wu, Elliptic curves in Huff's model, *http: //eprint.iacr.org/2010/390.pdf, 2010*,
4. R. Feng, M. Nie, and H. Wu., Twisted Jacobi intersections curves., *Theory and Applications of Models of Computation (2010), 199-210.*,
5. O. Billet, and M. Joye, The Jacobi model of an elliptic curve and side- channel analysis, *AAECC 2003, Lect. Notes in Comp. Scie.* ***2643*** *(2003), 34-42, Springer-Verlag*,
6. D. Bernstein, P. Birkner, M. Joye, T. Lange, C. Peters, Twisted Edwards curves, *Progress in cryptology-AFRICACRYPT 2008 proceed- ings, edited by S. Vaudenay, Lect. Notes in Comp. Scie.* ***5023*** *(2008),389-405, Springer.*,
7. René Schoof, Elliptic curves over finite fields and the computation of square roots mod p, *Math. Comp.****44*** *(1985), no. 170, 483–494.*,