



Université de Caen Basse-Normandie
Laboratoire GREYC



Proposition de stage d'initiation à la recherche :

Algorithmes de calculs de couplage sur les courbes elliptiques pour la cryptographie

Fabien LAGUILLAUMIE

<http://users.info.unicaen.fr/~flaguill/>

Lieu du stage :

Laboratoire GREYC

Université de Caen Basse-Normandie - Campus 2

Boulevard du Maréchal Juin - BP 5186

14032 Caen cedex - France

<https://www.greyc.fr/>

Durée du stage : 3 mois

Sujet : Dans le cadre du projet ANR PACE (<https://pace.rd.francetelecom.com/>) des membres de l'équipe Algorithmique du GREYC s'intéressent à l'implantation de l'algorithme Miller [Mil04] pour calculer des couplages sur les courbes elliptiques. Ces couplages sont des objets mathématiques qui ont permis de lever des verrous dans la conception de systèmes cryptographiques [Jou00, BF01] grâce à leur propriété de bilinéarité, compatible avec les exigences de sécurité de ces systèmes. Des avancées récentes en matière de preuves non-interactives [GS08, B+10] nécessitent une utilisation intensive des couplages, et l'efficacité de leur calcul devient crucial.

Un couplage e transforme un couple de points d'une courbe elliptique définie sur un certain corps dans le groupe multiplicatif d'un corps fini. Sa propriété essentielle de bilinéarité se traduit par le fait que $e(aP, bQ) = e(P, Q)^{ab}$ pour tous points P et Q et tous entiers a et b . L'algorithme de Miller permet de réaliser le calcul de ce couplage (l'évaluation d'une fonction rationnelle de la courbe en un diviseur) à la façon "square and multiply". Toutes les courbes elliptiques ne permettent pas d'implanter des couplages, seules les courbes dites "pairing-friendly" sont adaptées. Parmi ces courbes, trois types existent (qui dépendent des groupes de points sur lesquels agit le couplage), qui ont chacun des implications cryptographiques différentes.

L'objectif de ce stage est d'étudier plusieurs implantations de ces couplages, avec différentes courbes (et différents types) pour obtenir différentes propriétés nécessaires dans les applications cryptographiques. La partie développement se fera en C/C++.

Pour plus d'informations : fabien.laguillaumie@info.unicaen.fr.

Références

- [B+10] O. Blazy, G. Fuchsbauer, M. Izabachène, A. Jambert, H. Sibert and D. Vergnaud. *Batch Groth-Sahai*, Cryptology ePrint Archive, Report 2010/040, 2010. Available at : <http://eprint.iacr.org/2010/040>
- [BF01] D. Boneh and M. K. Franklin. *Identity-Based Encryption from the Weil Pairing*. Proc. of Crypto'01, Springer LNCS Vol. 2139, pp. 213–229 (2001)
- [GS08] J. Groth and A. Sahai. *Efficient non-interactive proof systems for bilinear groups*. Proc. of Eurocrypt'08, Springer LNCS Vol. 4965, 415–432 (2008)
- [Jou00] A. Joux : A One Round Protocol for Tripartite Diffie–Hellman. Proc.of ANTS IV, Springer LNCS Vol. 1838, 385–394 (2000)
- [Mil04] V. S. Miller. *The Weil Pairing, and Its Efficient Calculation*. J. Cryptology 17(4) : 235–261 (2004)