Bigou Karim
Doctorant DGA-INRIA
IRISA Équipe CAIRN (Lannion)

Directeur de thèse: Arnaud Tisserand
Co-directeur de thèse: Nicolas Guillermin

Avancées sur l'utilisation de la représentation RNS pour la cryptographie sur courbes elliptiques .

La question de la sécurité des dispositifs de cryptographie face aux attaques se pose à plusieurs niveaux. La sécurité au niveau théorique repose sur l'utilisation de structures mathématiques et de protocoles cryptographiques très robustes. Les implantations doivent aussi être protégées des « attaques par canaux cachés », par exemple les attaques sur la consommation d'énergie ou le rayonnement électromagnétique. Dans le cadre d'implantations matérielles pour la cryptographie, la représentation modulaire des nombres ou RNS (pour *Residue Number System*) s'est montrée comme une alternative intéressante ([1], [2], [3], [4]), en particulier pour les courbes elliptiques (ECC). La représentation RNS offre des perspectives intéressantes en matière de protection contre certaines attaques par canaux cachés, tout en étant très performante.

En RNS, un nombre est représenté par ses restes modulo un ensemble d'entiers premiers entre eux : la base RNS. Ce système de représentation est non positionnel, il n'y a pas de notion de poids ou d'ordre entre les moduli. Les opérations d'addition, de soustraction et de multiplication s'effectuent en parallèle sur chacun des moduli. Il n'y a pas de propagation de retenue entre ceux-ci. Cette caractéristique permet d'obtenir de hautes vitesses de calcul sur des grands nombres, de 160 à 600 bits pour ECC. En plus de l'aspect performance, l'indépendance des calculs sur les différents moduli permet aussi de choisir l'ordre des calculs internes. En particulier, une façon de brouiller les pistes peut être alors de rendre aléatoire l'ordre des calculs sur les différents moduli. La représentation RNS a néanmoins des inconvénients, certaines opérations comme la division et la comparaison sont bien plus complexes que dans les systèmes classiques positionnels.

L'objectif est de présenter l'arithmétique orientée pour les courbes elliptiques dans un corps fini premier en RNS, ainsi que les premiers résultats obtenus dans le cadre de ma thèse. Je commencerai par une brève introduction aux courbes elliptiques. Je présenterai ensuite le RNS, ses avantages et inconvénients, ainsi que les principaux algorithmes RNS utilisés et quelques astuces existantes. Enfin, je montrerai comment les opérations sur les courbes elliptiques sont effectuées dans cette représentation et comment j'ai pu accélérer une opération compliquée en RNS : l'inversion modulaire.

[1] S. Kawamura, M. Koike, F. Sano, and A. Shimbo. Cox-rower architecture for fast parallel montgomery multiplication. In Proc. 19th International Conference on the Theory and Application of Cryptographic (EUROCRYPT), volume 1807 of LNCS, pages 523–538, Bruges, Belgium, May 2000. Springer.

[2] J.-C. Bajard and L. Imbert. A full RNS implementation of RSA. IEEE Transactions on Computers, 53(6):769–774, June 2004.

[3] N. Guillermin. A high speed coprocessor for elliptic curve scalar multiplications over Fp. In Proc. Cryptographic Hardware and Embedded Systems (CHES), volume 6225 of LNCS, pages 48–64, Santa Barbara, CA, USA, August 2010. Springer.

[4] N. Guillermin. Implementation materielle de coprocesseurs haute performance pour la cryptographie asymetrique. Phd thesis, Universite Rennes 1, January 2012.