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

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

Cryptographie sur courbes elliptiques en représentation modulaire des nombres (RNS)

La question de la sécurité des dispositifs de cryptographie face à des 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. 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]), en particulier pour les courbes elliptiques (ECC). La représentation RNS offre des perspectives intéressantes en matière de protection contre les 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 (typiquement 160 à 600 bits pour ECC). En plus de l'aspect performance, ce parallélisme naturel permet aussi de choisir l'ordre des calculs effectués. Une façon de brouiller les pistes peut être alors de rendre aléatoire l'ordre des calculs sur les différents moduli. En contrepartie, certaines opérations comme la division et la comparaison sont bien plus complexes que dans des systèmes classiques positionnels. Dans la thèse de Nicolas Guillermin [3], l'implantation FPGA proposée s'avère très compétitive, notamment si le corps premier de base est quelconque.

Je propose de présenter le cadre dans lequel s'inscrit mon sujet de thèse. Je commencerai par une brève introduction aux courbes elliptiques et au principe des attaques par canaux cachés (une implantation matérielle est un des objectifs). Je présenterai ensuite le RNS, ses avantages et inconvénients, ainsi que des algorithmes RNS utilisés pour le calcul dans un corps premier. Enfin, je montrerai comment les opérations sur les courbes elliptiques sont effectuées dans cette représentation.

[1] S. Kawamura, M. Koike, F. Sano, and A. Shimbo. *Cox-Rower Architecture for Fast Parallel Montgomery Multiplication*. In Advances in Cryptology—EUROCRYPT 2000, pages 523–538. Springer, 2000.

[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. *Implémentation matérielle de coprocesseurs haute performance pour la cryptographie asymétrique*. Thèse Université Rennes 1. Jan. 2012