PMNS pour une arithmétique modulaire efficace, à faible coût mémoire

Fangan Yssouf Dosso,*Départment SAS*, École des Mines de Saint-Étienne
Jean-Marc Robert, Pascal Véron, *Laboratoire IMATH*, Université de Toulon

Le PMNS (Polynomial Modular Number System) est un système de représentation de nombres entiers qui vise à accélérer les opérations arithmétiques modulo un nombre premier p. Un tel système est défini par un tuple (p, n, g, r, E), où p, n, g et r sont des entiers positifs, et E un polynôme unitaire à coefficients entiers, ayant g comme racine modulo p. La plupart des travaux réalisés sur le PMNS se concentrent sur des binômes unitaires E, où le terme constant est un petit entier non nul (typiquement 2 ou -2), car un tel polynôme permet de construire des PMNS efficaces avec un faible coût mémoire. Cependant, un travail récent nous a permis d'observer que ces polynômes ne sont pas toujours les meilleurs choix.

Dans cette présentation, nous commençons par une présentation du PMNS, avec l'essentiel de l'arithmétique dans ce système. Ensuite, nous mettons en évidence un nouvel ensemble de polynômes E permettant la construction de PMNS très efficaces et avec un faible coût de représentation. Nous présentons également de nouveaux paramètres, avec de nouvelles bornes plus fines. Nous montrons que ces polynômes sont plus intéressants que (la plupart) des binômes. Pour finir, nous nous intéressons à l'utilisation du PMNS pour randomiser les opérations arithmétiques, afin de randomiser des opérations de haut niveau comme la multiplication scalaire sur courbe elliptique. Cela, pour protéger les implémentations contre certaines attaques par canaux auxiliaires avancées, comme la DPA (Differential Power Analysis).