Randomisation des opérations arithmétiques avec le PMNS

Laurent-Stéphane Didier, **Fangan Yssouf Dosso**, Nadia El Mrabet, Jérémy Marrez, Pascal Véron

Le PMNS (Polynomial Modular Number System) est un système de numération non positionnel qui permet d'effectuer les opérations arithmétiques modulo un entier p. Un tel système est défini par un tuple $\mathcal{B} = (p, n, \gamma, \rho, E)$, où p, n, γ et ρ sont des entiers positifs non nuls, et $E \in \mathbb{Z}_n[X]$, avec $E(\gamma) \equiv 0 \pmod{p}$. Dans un PMNS, un élément $a \in \mathbb{Z}/p\mathbb{Z}$ est représenté par un polynôme A tel que $A(\gamma) \equiv a \pmod{p}$, $\deg A < n$ et $\|A\|_\infty < \rho$; on dit alors que A est une représentation de a. Plusieurs travaux ont montré que ce système peut être une alternative intéressante au système de représentation classique pour l'arithmétique modulaire. Le PMNS est un système redondant. Cette redondance peut être exploitée pour randomiser les opérations dans ce système.

Dans cette présentation, nous nous intéresserons à la randomisation de certaines opérations dans le PMNS, afin de protéger les implémentations contre certaines attaques par canaux auxiliaires. Pour cela, nous verrons comment générer un PMNS tout en garantissant, pour chaque élément de $\mathbb{Z}/p\mathbb{Z}$, le nombre minimum de représentations distinctes que nous souhaitons dans ce PMNS. Puis, nous verrons comment atteindre de façon aléatoire chacune de ces représentations. Comme application, nous verrons comment randomiser la multiplication scalaire sur les courbes elliptiques.