Implantations de multiplications modulaires et exponentiations en lot utilisant l'extension IFMA52

Laurent-Stéphane Didier[1], Léa Glandus[1], and Jean-Marc Robert*[1]

[1]IAA/IMATH Université de Toulon – Université du Sud - Toulon - Var : EA2134 – France

Résumé

Nous présentons des expériences d'implantations de multiplications modulaires en lot utilisant l'extension IFMA52. Cette extension du jeu d'instructions x86-64 offre la possibilité d'effectuer 8 multiplications-additions simultanément avec des opérandes de 52 bits rangées dans 8 mots de 64 bits, dans des registres de 512 bits.
On explore dans cette configuration différentes tailles (jusqu'à 4096 bits) et différents algorithmes de multiplication (schoolbook ou Karatsuba).
Pour les tailles jusqu'à 4096 bits, on peut donc effectuer 8 multiplications en parallèle et, avec une réduction modulaire de Montgomery, implanter 8 exponentiations en lot parallèle. Le gain en performance en comparaison avec des bibliothèques de l'état de l'art (GMP ou OpenSSL) est significatif.

*Intervenant