Soumission de présentation
Journées Codage et Cryptographie 2012
du 7 au 12 octobre 2012, à Dinard

MULTIPLICATION SCALAIRE OPTIMISÉE SUR COURBES ELLIPTIQUES BINAIRES SUR INTEL CORE i7

Jean-Marc ROBERT (DALI/LIRMM, Perpignan)

Les calculs cryptographiques nécessitent d'effectuer des opérations sur des corps finis avec les règles arithmétiques correspondantes. Le développement de la cryptographie sur les courbes elliptiques (*ECC, Elliptic Curve Cryptography*), et plus particulièrement celles définies sur les corps binaires ($\mathbb{F}_{2^m}$), implique d'implémenter ces opérations à l'aide d'algorithmes de plus en plus performants, et de tirer parti des plates-formes disposant des processeurs ayant un jeu d'instruction étendu à l'arithmétique des polynômes de ces corps binaires.

Après avoir rappelé les fondements de l'arithmétique sur les courbes elliptiques ainsi que pour les opérations sur les corps binaires, nous parlerons ensuite d'optimisations du code exploitant les spécificités du processeur Intel Core I7, en particulier la multiplication sans retenue (*carry-less multiplier*), ainsi que l'utilisation des registres MMX (*MultiMedia eXtension*). Ces deux optimisations impliquent une refonte profonde de la façon de coder les algorithmes, de par le caractère *SIMD* du jeu d'instruction correspondant. Nous montrerons combien les algorithmes doivent être adaptés à de tels types de variables.

Ces implémentations permettent d'atteindre les meilleures performances publiées et d'être au niveau de l'état de l'art.

Peut-on aller plus loin ? Certaines combinaisons d'opérations sur le corps binaire ($\mathbb{F}_{2^m}$), lorsque des opérandes sont communes ou donnent lieu à des simplifications, peuvent-elles apporter un gain supplémentaire ? L'examen d'optimisations prenant en compte des opérations combinées de type AB, AC et $AB + CD$, $(A, B, C, D \in \mathbb{F}_{2^m})$ fait l'objet d'expérimentations. La combinatoire des cas (taille des corps binaires finis et type des variables manipulées par les implémentations) est partiellement explorée. Des gains sont observés sous certaines conditions.

Les expérimentations menées laissent encore la question ouverte, mais tracent la voie à des développements ultérieurs.