UMR IRISA

Stage L3 2011–2012

Titre : Compilation de circuits sécurisés pour la cryptographie sur les courbes elliptiques

Thématique : sécurité et cryptologie

Durée : 2 à 3 mois

Laboratoire : Laboratoire IRISA, équipe CAIRN, campus ENSSAT, 6 rue Kérampont, 22300 Lannion

Contact : Arnaud Tisserand, email : `mailto:arnaud.tisserand@irisa.fr`

Mots clés : cryptographie sur les courbes elliptiques, arithmétique, circuit intégré numérique, FPGA

Sujet

Un compilateur de circuits intégrés numériques pour la cryptographie sur les courbes elliptiques (ECC) est développé dans l'équipe CAIRN de l'IRISA. À partir d'une description mathématique des calculs requis pour une application ECC et d'une description de haut niveau de l'architecture du circuit, il produit le code VHDL optimisé d'un (co-)processeur autonome. Il utilise une bibliothèque d'algorithmes arithmétiques et de représentations des nombres et des points de la courbe. Différents objectifs peuvent être spécifiés pour orienter les phases de compilation :

- vitesse, débit, latence (niveau de parallélisme interne, pipeline) ;
- taille du circuit (pour le coût silicium) ;
- consommation d'énergie (choix des algorithmes et des représentations) ;
- sécurité par rapport à des attaques physiques.

Le stage portera sur la sécurisation du processeur face à certaines attaques par canaux cachés en analyse de la consommation d'énergie. Ces attaques utilisent la corrélation entre le secret (valeur des bits de la clé) et l'activité électrique du circuit (transitions des données ou parasites). Deux pistes sont envisageables : rendre l'activité du circuit indépendante du secret (courbes particulières, randomisation) ou bien limiter les variations d'activité (équilibrage des calculs, codages physiques spécifiques). Notre approche se situera au niveau des algorithmes arithmétiques et des représentations des données (aux niveaux du corps fini et de la courbe utilisés) et puis de leur codage physique dans le circuit. En particulier, les compromis entre la taille des opérateurs et le nombre d'unités de calcul disponibles en parallèle seront étudiés (multiples petites unités contre quelques unités très larges). Les résultats seront analysés expérimentalement en utilisant le banc d'attaques (sondes, oscilloscope numérique rapide et machine de traitement) et des cartes FPGA disponibles dans notre équipe. Les meilleurs algorithmes et représentations seront intégrés au compilateur.

Commentaires

Une indemnité de stage sera possible au tarif fixé par l'IRISA.

Références

- D. Hankerson, A. Menezes and S. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer, 2004, `http://www.cacr.math.uwaterloo.ca/ecc/`
- N. Weste and D. Harris. *CMOS VLSI Design : A Circuits and Systems Perspective*. Addison Wesley, 3rd edition, 2004, `http://www.cmosvlsi.com/`

Compétences espérées

Profile recherché : informaticien(ne) avec un intérêt pour la micro-électronique. Connaissances de base en cryptographie asymétrique, en arithmétique (corps finis) et en compilation. Des connaissances sur les circuits intégrés (FPGA en particulier) serait un avantage, mais elles peuvent être acquises pendant le stage.