Protection contre les attaques de type SPA pour la cryptographie sur courbes hyperelliptiques

Oumar Diao et Marc Joye

Résumé. Dans ce travail, nous présentons des formules d'addition unifiées sur les Jacobiennes de courbes hyperelliptiques de genre $g \geq 1$. Ces formules unifiées constituent une parade efficace contre les attaques par canaux auxiliaires de type SPA. Nos formules unifiées sont valables sur toute Jacobienne de courbes hyperelliptiques définie sur un corps quelconque. En particulier, dans le cas du genre 2, nous obtenons ainsi les formules explicites unifiées les plus efficaces, n'engendrant qu'un très léger surcoût par rapport aux meilleures formules explicites non unifiées.

Preventing SPA-type Attacks for Hyperelliptic Curve Cryptography

Oumar Diao and Marc Joye

Abstract. In this work, we present unified addition formulas for Jacobians of hyperelliptic curves of genus $g \geq 1$. These unified formulas provide an efficient protection against SPA-type side-channel attacks. Our unified formulas apply on any Jacobian of hyperelliptic curves defined over any field. In particular, for genus two, we so obtain the most efficient explicit unified formulas, only very slightly increasing the cost compared to the best explicit non-unified formulas.