The Interleaved Ladders: securing algorithms against side-channel and fault-injection attacks

Yoann Marquer*[1], Tania Richmond[2], and Pascal Véron[3]

[1]Inria Rennes – Bretagne Atlantique – Institut National de Recherche en Informatique et en Automatique – France
[2]DGA Maîtrise de l'information – DGA – France
[3]Laboratoire IMATH – , Université de Toulon – France

Résumé

The Montgomery ladder is an algorithm for the modular exponentiation (used in cryptosystems like RSA) and the scalar multiplication (used in elliptic-curve cryptography) which is secure regarding most timing and power side-channel attacks and some fault-injection attacks.
These desirable security properties are obtained from the code structure (an iterative conditional branching), and an interleaving of variables over iterations that preserves some invariant (and can also be used to detect fault-injection attacks).

We abstract away these properties as systems of equations, and obtained semi- and fully-Interleaved Ladders as a class of secure algorithms.

Indeed, these Interleaved Ladders are protected against most side-channel attacks, and we compare the vulnerability of the none-, semi- and fully-Interleaved Ladders regarding several fault-injection attacks.
Finally, we apply the semi- and fully-Interleaved Ladder equations to the modular exponentiation and the scalar multiplication cases to obtain novel and more secure algorithms, and we investigate their cost and feasibility.

*Intervenant