Interleaved Ladders: One More Step on Generalizing the Montgomery Ladder

Tania Richmond
Université de la Nouvelle Calédonie, Nouméa, France

Abstract

Instances of iterative conditional branching appear in various sensitive algorithms, like the modular exponentiation in the RSA cryptosystem or the scalar multiplication in elliptic-curve cryptography. The Montgomery ladder is a common example of such algorithm with desirable security properties against some side-channel and fault-injection attacks. Our approach represents the first systematic effort to define a formal framework that encompasses the Montgomery ladder within a more general class of algorithms satisfying these security properties. This framework is based on two systems of equations, one for the semi-interleaved ladders like the Montgomery ladder, and one for a generalization we call the fully-interleaved ladders. Furthermore, this innovative approach enables us to design new fault-injection attacks, capable of extracting some or all bits of the secret against various ladders, thereby compromising the conventional Montgomery ladder. We also validate the generality of our approach by applying our ladder equations to modular exponentiation and scalar multiplication, both in the semi- and fully-interleaved cases, to propose new, more secure algorithms, while the Montgomery ladder remains the optimal solution in terms of performance, thus leading to relevant trade-offs between ladder variants.

Keywords: Security, Cryptography, Side-channel attacks, Fault injection attacks, Modular Arithmetic, Interleaved Ladders