Cryptology ePrint Archive: Report 2011/170

Software implementation of binary elliptic curves: impact of the carry-less multiplier on scalar multiplication

Jonathan Taverne and Armando Faz-Hern\'andez and Diego F. Aranha and Francisco Rodr\'iguez-Henr\'iquez and Darrel Hankerson and Julio L\'opez

Abstract: The availability of a new carry-less multiplication instruction in the latest Intel desktop processors significantly accelerates multiplication in binary fields and hence presents the opportunity for reevaluating algorithms for binary field arithmetic and scalar multiplication over elliptic curves. We describe how to best employ this instruction in field multiplication and the effect on performance of doubling and halving operations. Alternate strategies for implementing inversion and half-trace are examined to restore most of their competitiveness relative to the new multiplier. These improvements in field arithmetic are complemented by a study on serial and parallel approaches for Koblitz and random curves, where parallelization strategies are implemented and compared. The contributions are illustrated with experimental results improving the state-of-the-art performance of halving and doubling-based scalar multiplication on NIST curves at the 112- and 192-bit security levels, and a new speed record for side-channel resistant scalar multiplication in a random curve at the 128-bit security level.

Category / Keywords: Elliptic curve cryptography, finite field arithmetic, parallel algorithm, efficient software implementation

Date: received 3 Apr 2011, last revised 13 Oct 2011

Contact author: francisco at cs cinvestav mx