Cryptology ePrint Archive: Report 2011/338

Fast and Regular Algorithms for Scalar Multiplication over Elliptic Curves

Matthieu Rivain

Abstract: Elliptic curve cryptosystems are more and more widespread in everyday-life applications. This trend should still gain momentum in coming years thanks to the exponential security enjoyed by these systems compared to the subexponential security of other systems such as RSA. For this reason, efficient elliptic curve arithmetic is still a hot topic for cryptographers. The core operation of elliptic curve cryptosystems is the scalar multiplication which multiplies some point on an elliptic curve by some (usually secret) scalar. When such an operation is implemented on an embedded system such as a smart card, it is subject to {\em side channel attacks}. To withstand such attacks, one must constrain the scalar multiplication algorithm to be {\em regular}, namely to have an operation flow independent of the input scalar. A large amount of work has been published that focus on efficient and regular scalar multiplication and the choice leading to the best performances in practice is not clear. In this paper, we look into this question for general-form elliptic curves over large prime fields and we complete the current state-of-the-art. One of the fastest low-memory algorithms in the current literature is the Montgomery ladder using co-Z Jacobian arithmetic {\em with X and Y coordinates only}. We detail the regular implementation of this algorithm with various trade-offs and we introduce a new binary algorithm achieving comparable performances. For implementations that are less constrained in memory, windowing techniques and signed exponent recoding enable reaching better timings. We survey regular algorithms based on such techniques and we discuss their security with respect to side-channel attacks. On the whole, our work give a clear view of the currently best time-memory trade-offs for regular implementation of scalar multiplication over prime-field elliptic curves.

Category / Keywords: implementation /

Date: received 22 Jun 2011, last revised 17 Aug 2011

Contact author: matthieu rivain at gmail com