Cryptology ePrint Archive: Report 2011/039

Fast Quadrupling of a Point in Elliptic Curve Cryptography

Duc-Phong Le

Abstract: Ciet et al. proposed a very elegant method for trading inversions for multiplications when computing $2P + Q$ from given points P and Q on elliptic curves of Weierstrass form. In this paper we extend their method and present a fast algorithm for computing $4P$ with only one inversion in affine coordinates. Our algorithm is faster than two repeated doublings whenever the cost of one field inversion is more expensive than the cost of four field multiplications plus three field squarings (i.e. ${\sf I > 4M + 4S}$). It saves one filed multiplication and one field squaring in comparison with Sakai-Sakurai's method. We also show that on particular curves (i.e. $a = 0$ or $b = 0$), our algorithm gains better results.

Category / Keywords: Elliptic curve cryptography, fast arithmetic, affine coordinates

Date: received 20 Jan 2011, last revised 7 Nov 2011

Contact author: tslld at nus edu sg