Cryptology ePrint Archive: Report 2011/315

Implementing 4-Dimensional GLV Method on GLS Elliptic Curves with j-Invariant 0

Zhi Hu and Patrick Longa and Maozhi Xu

Abstract: The Gallant-Lambert-Vanstone (GLV) method is a very efficient technique for accelerating point multiplication on elliptic curves with efficiently computable endomorphisms. Galbraith, Lin and Scott (J. Cryptol. 24(3), 446-469 (2011)) showed that point multiplication exploiting the 2-dimensional GLV method on a large class of curves over GF(p^2) was faster than the standard method on general elliptic curves over GF(p), and left as an open problem to study the case of 4-dimensional GLV on special curves (e.g., j(E) = 0) over GF(p^2). We study the above problem in this paper. We show how to get the 4-dimensional GLV decomposition with proper decomposed coefficients, and thus reduce the number of doublings for point multiplication on these curves to only a quarter. The resulting implementation shows that the 4-dimensional GLV method on a GLS curve runs in about 0.78 the time of the 2-dimensional GLV method on the same curve and in between 0.78-0.87 the time of the 2-dimensional GLV method using the standard method over GF(p). In particular, our implementation reduces by up to 27% the time of the previously fastest implementation of point multiplication on x86-64 processors due to Longa and Gebotys (CHES2010).

Category / Keywords: public-key cryptography / Elliptic curves, point multiplication, GLV method, GLS curves.

Publication Info: Full version of a journal paper to appear in Designs, Codes and Cryptography

Date: received 15 Jun 2011, last revised 17 Oct 2011

Contact author: plonga at microsoft com