Cryptology ePrint Archive: Report 2011/608

Four-Dimensional Gallant-Lambert-Vanstone Scalar Multiplication

Patrick Longa and Francesco Sica

Abstract: The GLV method of Gallant, Lambert and Vanstone~(CRYPTO 2001) computes any multiple kP of a point P of prime order n lying on an elliptic curve with a low-degree endomorphism Φ (called GLV curve) over $\mathbb{F}_p$ as $kP = k_1P + k_2\Phi(P)$, with $\max\{|k_1|,|k_2|\}\leq C_1\sqrt n$ for some explicit constant $C_1>0$. Recently, Galbraith, Lin and Scott (EUROCRYPT 2009) extended this method to all curves over $\mathbb{F}_{p^2}$ which are twists of curves defined over $\mathbb{F}_p$. We show in this work how to merge the two approaches in order to get, for twists of any GLV curve over $\mathbb{F}_{p^2}$, a four-dimensional decomposition together with fast endomorphisms Φ, Ψ over $\mathbb{F}_{p^2}$ acting on the group generated by a point P of prime order n, resulting in a proven decomposition for any scalar $k\in[1,n]$ given by $kP=k_1P+ k_2\Phi(P)+ k_3\Psi(P) + k_4\Psi\Phi(P)$, with $\max_i (|k_i|)< C_2\, n^{1/4}$ for some explicit $C_2>0$. Remarkably, taking the best C_1, C_2, we obtain $C_2/C_1<412$, independently of the curve, ensuring in theory an almost constant relative speedup. In practice, our experiments reveal that the use of the merged GLV-GLS approach supports a scalar multiplication that runs up to 50\% faster than the original GLV method. We then improve this performance even further by exploiting the Twisted Edwards model and show that curves originally slower may become extremely efficient on this model. In addition, we analyze the performance of the method on a multicore setting and describe how to efficiently protect GLV-based scalar multiplication against several side-channel attacks. Our implementations improve the state-of-the-art performance of point multiplication for a variety of scenarios including side-channel protected and unprotected cases with sequential and multicore execution.

Category / Keywords: Elliptic curves, GLV-GLS method, scalar multiplication, Twisted Edwards curve, side-channel protection, multicore computation.

Publication Info: This is the full version of a paper accepted to ASIACRYPT 2012.

Date: received 9 Nov 2011, last revised 12 Sep 2012

Contact author: plonga at microsoft com