Cryptology ePrint Archive: Report 2011/608

Four-Dimensional Gallant-Lambert-Vanstone Scalar Multiplication

Peter Birkner and 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 \[kP = k_1P + k_2\Phi(P), \quad\text{with } \max\{|k_1|,|k_2|\}\leq C_1\sqrt n \] 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 proved decomposition for any scalar $k\in[1,n]$ $$ kP=k_1P+ k_2\Phi(P)+ k_3\Psi(P) + k_4\Psi\Phi(P)\quad \text{with } \max_i (|k_i|) < C_2\, n^{1/4} $$ for some explicit $C_2>0$. Furthermore, taking the best C_1, C_2, we get $C_2/C_1<408$, independently of the curve, ensuring a constant relative speedup.

We also derive new families of GLV curves, corresponding to those curves with degree 3 endomorphisms.

Category / Keywords: implementation / Elliptic curves, GLV scalar multiplication, GLV curves

Date: received 9 Nov 2011, last revised 16 Nov 2011

Contact author: fracrypto at gmail com

Available formats: PDF | BibTeX Citation

Note: Corrected typos in the proof of Lemma 5.

Version: 20111116:182546 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]