International J. of Pure & Engg. Mathematics (IJPEM)
ISSN 2348-3881, Vol. 3 No. I (April, 2015), pp. 207-227

IMPROVING THE UPPER BOUNDS OF THE GALLAND, LAMBERT AND VANSTONE METHOD : THE THEORETICAL ASPECTS

RUMA KAREEM K. AJEENA
Babylon University, Department of Mathematics,
Mathematics School, Babil City, Iraq

Abstract

Gallant, Lambert and Vanstone (GLV) method is a generic algorithm which uses an efficiently computable endomorphism ψ to compute any multiple kP of a point P of order n lying on an elliptic curve E. In this work, an accurate analysis of the GLV method has been introduced. This analysis optimizes and proves existing the upper bounds of GLV reduction map. The upper bounds determine the values C_i for $i = 1, 2$, which are greater than 1, in two cases. These cases are determined based on embedding the endomorphism rings $End(E)$. When $End(E)$ is embedded into integers ring $\mathbb{Z}$, the value C_i for $i = 2$ is equal to $\sqrt{1 + |\lambda|}$ where $\lambda \in [1, n-1]$. Whereas, the value C_i for $i = 1$ is equal to $\sqrt{1 + |w| + z}$ with w and z are small fixed integers when the embedding occurs on an imaginary quadratic field $\mathbb{Q}[\sqrt{D}]$ where D is a discriminant of the characteristic polynomial $p(X)$. With new upper bound of the GLV method that depends on the value C_i for $i = 2$, most percentage of the successful computation of scalar multiplication kP has been determined.

––––––––––––––––––––––––––––

Key Words : *Elliptic Curve Cryptography, Scalar Multiplication, GLV method, Efficiently computable endomorphism, Upper bounds.*

2000 AMS Subject Classification : Primary-11Dxx, 11Rxx, Secondary-20Gxx, 06Bxx.