Cryptology ePrint Archive: Report 2013/146

High-Performance Scalar Multiplication using 8-Dimensional GLV/GLS Decomposition

Joppe W. Bos and Craig Costello and Huseyin Hisil and Kristin Lauter

Abstract: This paper explores the potential for using genus~2 curves over quadratic extension fields in cryptography, motivated by the fact that they allow for an 8-dimensional scalar decomposition when using a combination of the GLV/GLS algorithms. Besides lowering the number of doublings required in a scalar multiplication, this approach has the advantage of performing arithmetic operations in a 64-bit ground field, making it an attractive candidate for embedded devices. We found cryptographically secure genus 2 curves which, although susceptible to index calculus attacks, aim for the standardized 112-bit security level. Our implementation results on both high-end architectures (Ivy Bridge) and low-end ARM platforms (Cortex-A8) highlight the practical benefits of this approach.

Category / Keywords: implementation / GLV, GLS, Genus 2

Date: received 11 Mar 2013

Contact author: jbos at microsoft com