Cryptology ePrint Archive: Report 2011/578

ACCELERATING THE SCALAR MULTIPLICATION ON GENUS 2 HYPERELLIPTIC CURVE CRYPTOSYSTEMS

Balasingham Balamohan

Abstract: Elliptic Curve Cryptography (ECC) was independently introduced by Koblitz and Miller in the eighties. ECC requires shorter sizes of underlying finite fields in com- parison to other public key cryptosystems such as RSA, introduced by Rivest, Shamir and Adleman. Hyperelliptic curves, a generalization of elliptic curves, require decreas- ing field size as genus increases. Hyperelliptic curves of genus g achieve equivalent security of ECC with field size 1/g times the size of field of ECC for g <= 4. Recently, a lot of research is being focused on increasing the efficiency of hyperelliptic curve cryptosystems (HECC). The most time consuming operation in HECC is the scalar multiplication. At present, scalar multiplication on HECC over prime fields under performs in terms of computational time compared to ECC of equivalent security. This thesis focuses on optimizing HECC scalar multiplication at the point arithmetic level. At the point arithmetic level we obtain more efficient doubling and mixed addi- tion operations to decrease the computational time in the scalar multiplication using binary expansions of scalars. In addition, we introduce tripling operations for the Jacobians of hyperelliptic curves to make use of multibase representations of scalars that are being used effectively in ECC. We also develop double-add operations for semi-affine coordinates and Lange’s new coordinates. We use these double-add opera- tions to improve the computational cost of precomputation for semi-affine coordinates and that of more important main phase of scalar multiplication for semi-affine coor- dinates and Lange’s new coordinates. We derive special addition to improve the cost of precomputation for Lange’s new coordinates and projective coordinates.

Category / Keywords: public-key cryptography / hyperelliptic curve cryptosystem, public-key cryptography,discrete logarithm problem

Publication Info: University of Ottawa Master of Computer Science Thesis

Date: received 25 Oct 2011

Contact author: bbala078 at uottawa ca

Available formats: PDF | BibTeX Citation

Version: 20111102:203813 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]