Cryptology ePrint Archive: Report 2011/468

Faster Scalar Multiplication on Ordinary Weierstrass Elliptic Curves over Fields of Characteristic Three

Hongfeng Wu and Chang-An Zhao

Abstract: This paper proposes new explicit formulae for the point doubling, tripling and addition on ordinary Weierstrass elliptic curves over finite fields of characteristic three. The cost of basic point operations is lower than that of all previously proposed ones. The new doubling, mixed addition and tripling formulae in projective coordinates require 3M+2C, 8M+1C+1D and 4M+4C+1D respectively, where M, C and D is the cost of a field multiplication, a cubing and a multiplication by a constant. We also provide the unified and complete group laws. Finally, we present several examples of ordinary elliptic curves in characteristic three for high security levels.

Category / Keywords: Elliptic curve, scalar multiplication, unified addition, cryptography, explicit formulae

Date: received 29 Aug 2011, last revised 4 Sep 2011

Contact author: whfmath at gmail com