Cryptology ePrint Archive: Report 2013/015

Complete and Unified Group Laws are not Enough for Elliptic Curve Cryptography

Graham Enos

Abstract: We analyze four recently proposed normal forms for elliptic curves. Though these forms are mathematically appealing and exhibit some cryptographically desirable properties, they nonetheless fall short of cryptographic viability, especially when compared to various types of Edwards Curves. In this paper, we present these forms and demonstrate why they fail to measure up to the standards set by Edwards Curves.

Category / Keywords: public-key cryptography / elliptic curve cryptosystem, Edwards Curves

Date: received 9 Jan 2013

Contact author: genos at uncc edu