Cryptology ePrint Archive: Report 2011/206

Isomorphism classes of Edwards curves over finite fields

R. Farashahi and D. Moody and H. Wu

Abstract: Edwards curves are an alternate model for elliptic curves, which have attracted notice in cryptography. We give exact formulas for the number of $\Fq$-isomorphism classes of Edwards curves and twisted Edwards curves. This answers a question recently asked by R. Farashahi and I. Shparlinski.

Category / Keywords: Elliptic curves, Edwards curves, Isomorphisms

Date: received 25 Apr 2011, last revised 17 Oct 2011

Contact author: dbmoody25 at gmail com