

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 \mathbb{F}_q -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

Available formats: [PDF](#) | [BibTeX Citation](#)

Note: After submission, we (Moody and Wu) became aware of independent work by R. Farashahi which has similar results. We have combined our work into this one article, so there will not be duplicate work in the literature.

Version: 20111017:155421 ([All versions of this report](#))

Discussion forum: [Show discussion](#) | [Start new discussion](#)

[[Cryptology ePrint archive](#)]