Cryptology ePrint Archive: Report 2011/135

On isogeny classes of Edwards curves over finite fields

Omran Ahmadi and Robert Granger

Abstract: We count the number of isogeny classes of Edwards curves over finite fields, answering a question recently posed by Rezaeian and Shparlinski. We also show that each isogeny class contains a {\em complete} Edwards curve, and that an Edwards curve is isogenous to an {\em original} Edwards curve over $\F_q$ if and only if its group order is divisible by 8 if $q \equiv -1 \pmod{4}$, and 16 if $q \equiv 1 \pmod{4}$. Furthermore, we give formulae for the proportion of $d \in \F_q \setminus \{0,1 \}$ for which the Edwards curve E_d is complete or original, relative to the total number of d in each isogeny class.

Category / Keywords: public-key cryptography / number theory

Publication Info: preprint

Date: received 16 Mar 2011, last revised 17 Mar 2011

Contact author: rgranger at computing dcu ie