Cryptology ePrint Archive: Report 2011/430

Analogues of Velu's formulas for Isogenies on Alternate Models of Elliptic Curves

Dustin Moody and Daniel Shumow

Abstract: Isogenies of elliptic curves have been well-studied, in part because there are several cryptographic applications. Using Velu's formula, isogenies can be evaluated explicitly given their kernel. However, Velu's formula applies to elliptic curves given by a Weierstrass equation. In this paper we show how to similarly evaluate isogenies on Edwards curves and Huff curves. Edwards and Huff curves are new normal forms for elliptic curves, different than the traditional Weierstrass form.

Category / Keywords: Elliptic curves; Isogenies; Edwards Curves; Huff curves

Date: received 9 Aug 2011, last revised 19 Oct 2011

Contact author: dbmoody25 at gmail com