Cryptology ePrint Archive: Report 2013/142

A NEW METHOD OF CHOOSING PRIMITIVE ELEMENTS FOR BREZING-WENG FAMILIES OF PAIRING FRIENDLY ELLIPTIC CURVES

Kisoon YOON

Abstract: In this paper we present a new method of choosing primitive elements for Brezing-Weng families of pairing friendly elliptic curves with small rho-value, and we improve on previously-known best rho-values of families for the cases k=16, 22, 28 and 46. Our construction uses fixed discriminants.

Category / Keywords: public-key cryptography / elliptic curves, finite fields, pairing-based cryptography

Date: received 8 Mar 2013

Contact author: kisoon yoon at unicaen fr