Cryptology ePrint Archive: Report 2011/040

Simple and Exact Formula for Minimum Loop Length in Ate_i Pairing based on Brezing-Weng Curves

Hoon Hong, Eunjeong Lee, Hyang-Sook Lee and Cheol-Min Park

Abstract: We provide a simple and exact formula for the minimum Miller loop length in Ate_i pairing based on Brezing-Weng curves, in terms of the involved parameters, under a mild condition on the parameters. It will be also shown that almost all cryptographically useful parameters satisfy the mild condition. Hence the simple and exact formula is valid for them. It will also turn out that the formula depends only on two parameters, providing freedom to choose the other parameters to address the design issues other than minimizing the loop length.

Category / Keywords: public-key cryptography / elliptic curve cryptosystem, pairing, number theory

Date: received 21 Jan 2011, last revised 21 Jan 2011

Contact author: ejlee127 at ewha ac kr