CORR 2001-31

Solving Elliptic Curve Discrete Logarithm Problems using Weil Descent

Michael Jacobson*, Alfred Menezes, Andreas Stein*

Abstract We provide a concrete instance of the discrete logarithm problem on an elliptic curve over $\mathbb{F}_{2^{155}}$ which resists all previously known attack methodology of Frey. We report on our implementation of index-calculus methods for hyperelliptic curves over characteristic two finite fields, and discuss the cryptographic implications of our results.