CORR 2001-68

Elliptic Curves with Compact Parameters

Ezra Brown*, Bruce T. Myers*, Jerome A. Solinas*

Abstract We present a family of elliptic curves, suitable for cryptographic use, whose parameters can be specified in a highly efficient way. This is done via complex multiplication and identity-based parameters. Some novel computational shortcuts for these families are also presented.

Keywords elliptic curves, certificates, public-key cryptography, complex multiplication, identity based.