CORR 99-46

Improved Algorithms for Arithmetic on Anomalous Binary Curves

Jerome A. Solinas*

Abstract It has become increasingly common to implement discrete-logarithm based public-key protocols on elliptic curves over finite fields. The basic operation is *scalar multiplication:* taking a given integer multiple of a given point on the curve. The cost of the protocols depends on that of the elliptic scalar multiplication operation.

Koblitz introduced a family of curves which admit especially fast elliptic scalar multiplication. His algorithm was later modified by Meier and Staffelbach. We give an improved version of the algorithm which runs 50new kind of representation of an integer, analogous to certain kinds of binary expansions. We also outline further speedups using precomputation and storage.

Keywords elliptic curves, exponentiation, public-key cryptography.