CORR 2000-53

Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms

R. Gallant*, R. Lambert*, & S. Vanstone

Abstract The fundamental operation in elliptic curve cryptographic schemes is that of point multiplication of an elliptic point by an integer. This paper describes a new method for accelerating this operation on classes of elliptic curves that have efficiently-computable endomorphisms. One advantage of the new method is that it is applicable to a larger class of curves than previous such methods.