CORR 2001-41

Low-Weight Binary Representations for Pairs of Integers

jerome A. Solinas

Abstract Shamir's method speeds up the computation of the product of powers of two elements of a group, a common object in public-key algorithms. Shamir's method is based on binary expansions and was designed for modular and finite field arithmetic. Elliptic curve arithmetic uses signed binary expansions rather than the ordinary binary expansions of modular arithmetic. This note extends Shamir's method to the elliptic curve setting by specifying an optimal signed binary representation for a pair of positive integers.