CORR 99-06

Analysis of the Xedni Calculus Attack

Michael J. Jacobson, Neal Koblitz*, Joseph H. Silverman*, Andreas Stein, and Edlyn Teske

Abstract The xedni calculus attack on the elliptic curve discrete logarithm problem (ECDLP) involves lifting points from the finite field $\mathbb{F}_p$ to the rational numbers $\mathbb{Q}$ and then constructing an elliptic curve over $\mathbb{Q}$ that passes through them. If the lifting points are linearly dependent, then the ECDLP is solved. Our purpose is to analyze the practicality of this algorithm. We find that asymptotically the algorithm is virtually certain to fail, because of an absolute bound on the size of the coefficients of a relation satisfied by the lifted points. Moreover, even for smaller values of p experiments show that the odds against finding a suitable lifting are prohibitively high.