CORR 2002-05

Obstacles to the Torsion-Subgroup Attack on the Decision Diffie-Hellman Problem

Neal Koblitz*, Alfred J. Menezes

Abstract The authors of [3] show that if one is given an elliptic curve, depending on a prime p, that is defined over a number field and has certain properties, then one can solve the Decision Diffie-Hellman Problem (DDHP) in $\mathbb{F}_p^*$ in prolynomial time. We show that it is unlikely that an elliptic curve with the desired properties exists.

Keywords Discrete Lograithm, Diffie-Hellman Problem, Elliptic Curve, Torsion Point, Modular Curve