CORR 2002-02

Factoring $N = pq^2$ with the Elliptic Curve Method

Peter Ebinger*, Edlyn Teske

Abstract Various cryptosystems have been proposed whose security relies on the difficulty of factoring integers of the special form $N = pq^2$. To factor integers of that form, Peralta and Okamoto introduced a variation of Lenstra's Elliptic Curve Method (ECM) of factorization, which is based on the fact that the Jacobi symbols $(\frac{a}{N})$ and $(\frac{a}{p})$ agree for all integers a coprime with q. We report on an implementation and extensive experiments with that variation, which have been conducted in order to determine the speed-up compared with ECM for numbers of general form.