# CORR 2000-48

## Analysis of the Weil Descent Attack of Gaudry, Hess and Smart

**Alfred Menezes & Minghua Qu***

**Abstract** We analyze the Weil descent attack of Gaudry, Hess and Smart [12] on teh elliptic curve discrete logarithm problem for elliptic curves defined over $\mathbb{F}_{2^n}$, where $n$ is prime.