

**CORR 99-58**

**Computing Discrete Logarithms in Quadratic Orders**

**Michael J. Jacobson, Jr.**

**Abstract** We present efficient algorithms for computing discrete logarithms in the class group of a quadratic order and for principality testing in a real quadratic order, based on the work of Düllmann and Abel. We show how the idea of generating relations with sieving can be applied to improve the performance of these algorithms. Computational results are presented which demonstrate that our new techniques yield a significant increase in the sizes of discriminants for which these discrete logarithm problems can be solved.