Cryptology ePrint Archive: Report 2013/147

A note on the practical complexity of the NFS in the medium prime case: Smoothness of Norms

Naomi Benger and Manuel Charlemagne and Kefei Chen

Abstract: During an ongoing examination of the behaviour, in practice, of the Number Field Sieve (NFS) in the medium prime case we have noticed numerous interesting patterns. In this paper we present findings on run-time observations of an aspect of the sieving stage. The contributions of these observations to the computational mathematics community are twofold: firstly, they bring us a step closer to understanding the true practical effectiveness of the algorithm and secondly, they enabled the development of a test for the effectiveness of the polynomials used in the NFS. The results of this work are of particular interest to cryptographers: the run-time of the NFS determines directly the security level of some discrete logarithm problem based protocols, such as those arising in pairing-based cryptography.

Category / Keywords: public-key cryptography / DLP, NFS, pairing based cryptography

Date: received 12 Mar 2013, last revised 2 Apr 2013

Contact author: charlem at sjtu edu cn