Cryptology ePrint Archive: Report 2012/720

Faster index calculus for the medium prime case. Application to 1175-bit and 1425-bit finite fields

Antoine Joux

Abstract: Many index calculus algorithms generate multiplicative relations between smoothness basis elements by using a process called {\it Sieving}. This process allows to filter potential candidate relations very quickly, without spending too much time to consider bad candidates. However, from an asymptotic point of view, there is not much difference between sieving and straightforward testing of candidates. The reason is that even when sieving, some small amount time is spend for each bad candidates. Thus, asymptotically, the total number of candidates contributes to the complexity.

In this paper, we introduce a new technique: {\it Pinpointing}, which allows us to construct multiplicate relations much faster, thus reducing the asymptotic complexity of relations' construction. Unfortunately, we only know how to implement this technique for finite fields which contain a medium-sized subfield. When applicable, this method improves the asymptotic complexity of the index calculus algorithm in the cases where the sieving phase dominates. In practice, it gives a very interesting boost to the performance of state-of-the-art algorithms. We illustrate the feasability of the method with a discrete logarithm record in medium prime finite fields of sizes 1175~bits and 1425~bits.

Category / Keywords: foundations / Discrete Logarithms, Medium prime field, Index calculus, Improved sieving

Date: received 24 Dec 2012, last revised 7 Jan 2013

Contact author: antoine joux at m4x org