Cryptology ePrint Archive: Report 2013/074

On the Function Field Sieve and the Impact of Higher Splitting Probabilities: Application to Discrete Logarithms in $\F_{2^{1971}}$

Faruk Gologlu and Robert Granger and Gary McGuire and Jens Zumbragel

Abstract: In this paper we propose a binary field variant of the Joux-Lercier medium-sized Function Field Sieve, which results not only in complexities as low as $L_{q^n}(1/3,2/3)$ for computing arbitrary logarithms, but also in an heuristic {\em polynomial time} algorithm for finding the discrete logarithms of degree one elements. To illustrate the efficiency of the method, we have successfully solved the DLP in the finite field with 2^{1971} elements.

Category / Keywords: DLP

Publication Info: Submitted

Date: received 15 Feb 2013, last revised 20 Feb 2013

Contact author: robbiegranger at gmail com