Cryptology ePrint Archive: Report 2013/071

Relation collection for the Function Field Sieve

Jérémie Detrey and Pierrick Gaudry and Marion Videau

Abstract: In this paper, we focus on the relation collection step of the Function Field Sieve (FFS), which is to date the best algorithm known for computing discrete logarithms in small-characteristic finite fields of cryptographic sizes. Denoting such a finite field by GF(p^n), where p is much smaller than n, the main idea behind this step is to find polynomials of the form a(t)-b(t)x in GF(p)[t][x] which, when considered as principal ideals in carefully selected function fields, can be factored into products of low-degree prime ideals. Such polynomials are called "relations", and current record-sized discrete-logarithm computations need billions of those.

Collecting relations is therefore a crucial and extremely expensive step in FFS, and a practical implementation thereof requires heavy use of cache-aware sieving algorithms, along with efficient polynomial arithmetic over GF(p)[t]. This paper presents the algorithmic and arithmetic techniques which were put together as part of a new public implementation of FFS, aimed at medium- to record-sized computations.

Category / Keywords: implementation / function field sieve; discrete logarithm; polynomial arithmetic; finite-field arithmetic

Publication Info: To be presented at ARITH 2013.

Date: received 14 Feb 2013

Contact author: Jeremie Detrey at loria fr