AURORE GUILLEVIC, University of Calgary and PIMS-CNRS

Computing discrete logarithms in non-prime finite fields

Computing discrete logarithms in finite fields is a main concern in cryptography. The best algorithms known are the Number Field Sieve and its variants in medium- and large-characteristic fields (e.g. $GF(p^2)$, $GF(p^{12})$); the Function Field Sieve and the Quasi Polynomial-time Algorithm in small characteristic finite fields (e.g. $GF(2^{4404})$). The last step a.k.a. the initial splitting step of the NFS and FFS algorithms computes a smooth decomposition of a given target. While new improvements have been made to reduce the complexity of the dominating relation collection and linear algebra steps of NFS and FFS, resulting in a smaller database of known logarithms of small elements, the target is still any large element of the finite field, so that finding a smooth enough decomposition over the database becomes harder.

Our present method applies to any finite field of composite extension degree. It exploits the available subfields with a cheap (polynomial-time) linear algebra step, resulting in a much more smooth decomposition of the target. This leads to a new trade-off in the asymptotic complexity of the initial splitting step: it is improved by a factor 2 in the exponent with FFS and $2^{1/3}$ in the exponent with NFS, for any finite field of even extension degree, and with a much smaller smoothness bound. In medium and large characteristic, it can be combined with Pomerance's Early Abort strategy. In small characteristic, it replaces the Waterloo algorithm of Blake, Fuji-Hara, Mullin and Vanstone. Moreover it reduces the width and the height of the following decreasing tree.