Data structures for parallel exponentiation in finite fields

Michael Nöcker

Finite fields $\mathbb{F}_{q^n}$, in particular those of characteristic 2, play an important rôle in many nowadays applications, including modern cryptography. The question how to represent a finite field is one of the keys for a successful implementation.

The work in hands discusses this question on the background of parallel exponentiation. Exponentiation is the basic arithmetic behind a family of public key cryptosystems that is based on the discrete logarithm problem. The starting point is an extended model of addition chains. This model contains two different types of steps. An attached weight to each of these steps takes the basic arithmetic properties of a chosen basis representation of $\mathbb{F}_{q^n}$ into account. We develop a new algorithm for parallel exponentiation and prove a new lower bound on this task in this model. Both approaches identify the weight as a key to pre-estimate the potential improvement of a basis representation when using parallel computing.

We discuss different versions of the two common types of basis for $\mathbb{F}_{q^n}$: polynomial and normal bases. In particular, we develop algorithms for normal elements that are generated by general Gauß periods. A new algorithm integrates fast polynomial multiplication and the free computation of the Frobenius automorphism for prime power Gauß periods. This approach generalizes an algorithm for prime Gauß periods. Another new tool, called decomposable Gauß periods, helps to extend the result to all finite fields for which normal general Gauß period exist. A normal basis representation due to such a Gauß period proves to be best for massive parallel exponentiation in finite fields.

All key algorithms have all been implemented and compared by experiments. A new scalable algorithm for parallel exponentiation summarizes all discussed ideas. It shows how fast polynomial multiplication and powerful parallel computing can work together successfully if normal Gauß periods are the linking basis representation.