Abstract

This paper is an extensive study of the issues of efficient software implementation of low genus hyperelliptic Jacobians over binary fields.

We first give a detailed description of the methods by which one obtains explicit formul from Cantors algorithm. We then present improvements on the best known explicit formul for curves of genus three and four. Special routines for multiplying vectors of field elements by a fixed quantity (which are much faster than performing the multiplications separately) are also deployed, and the explicit formul for all genera are redesigned or re-implemented accordingly.

To allow a fair comparison of the curves of different genera, we use a highly optimized software library for arithmetic in binary fields. Our goals in its development were to minimize the overheads and performance penalties associated to granularity problems, which have a larger impact as the genus of the curves increases. The current state of the art in attacks against the discrete logarithm problem is taken into account for the choice of the field and group sizes and performance tests are done on a personal computer.

Our results can be shortly summarized as follows: Curves of genus three provide performance similar, or better, to that of curves of genus two, and these two types of curves perform consistently around 50genus four attain a performance level comparable to, and more often than not, better than, elliptic curves. A large choice of curves is therefore available for the deployment of curve based cryptography, with curves of genus three and four providing their own advantages as larger cofactors can be allowed for the group order.