Cryptology ePrint Archive: Report 2011/306

Group Law Computations on Jacobians of Hyperelliptic Curves

Craig Costello and Kristin Lauter

Abstract: We derive an explicit method of computing the composition step in Cantor's algorithm for group operations on Jacobians of hyperelliptic curves. Our technique is inspired by the geometric description of the group law and applies to hyperelliptic curves of arbitrary genus.

While Cantor's general composition involves arithmetic in the polynomial ring $F_q[x]$, the algorithm we propose solves a linear system over the base field which can be written down directly from the Mumford coordinates of the group elements.

We apply this method to give more efficient formulas for group operations in both affine and projective coordinates for cryptographic systems based on Jacobians of genus 2 hyperelliptic curves in general form.

Category / Keywords: Hyperelliptic curves, group law, Jacobian arithmetic, genus 2.

Date: received 8 Jun 2011, last revised 19 Sep 2011

Contact author: craig costello at qut edu au