Cryptology ePrint Archive: Report 2011/306

Geometric Group Law Computations on Jacobians of Hyperelliptic Curves

Craig Costello and Kristin Lauter

Abstract: We derive a new 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. One advantage to our approach is that we get explicit formulas for composition without unrolling the loop in Cantor's algorithm which includes steps operating on polynomials in F_q[x] such as the Chinese Remainder Theorem. We 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. We also examine several other consequences of utilizing the geometric picture of Jacobian arithmetic for various genera.

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

Date: received 8 Jun 2011

Contact author: craig costello at qut edu au

Available formats: PDF | BibTeX Citation

Version: 20110609:114524 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]