Cryptology ePrint Archive: Report 2011/105

Explicit Formulas for Real Hyperelliptic Curves of Genus 2 in Affine Representation

S. Erickson and M. J. Jacobson, Jr. and A. Stein

Abstract: We present a complete set of efficient explicit formulas for arithmetic in the degree 0 divisor class group of a genus two real hyperelliptic curve given in affine coordinates. In addition to formulas suitable for curves defined over an arbitrary finite field, we give simplified versions for both the odd and the even characteristic cases. Formulas for baby steps, inverse baby steps, divisor addition, doubling, and special cases such as adding a degenerate divisor are provided, with variations for divisors given in reduced and adapted basis. We describe the improvements and the correctness together with a comprehensive analysis of the number of field operations for each operation. Finally, we perform a direct comparison of cryptographic protocols using explicit formulas for real hyperelliptic curves with the corresponding protocols presented in the imaginary model.

Category / Keywords: foundations / hyperelliptic curve, reduced divisor, infrastructure and distance, Cantor's algorithm, explicit formulas, efficient implementation, cryptographic key exchange

Publication Info: Submitted to Advances in Mathematics of Communication

Date: received 2 Mar 2011

Contact author: jacobs at cpsc ucalgary ca