

1035-11-669

Stefan Erickson* (Stefan.Erickson@ColoradoCollege.edu), Department of Mathematics & Computer Science, Colorado College, 14 E. Cache La Poudre St., Colorado Springs, CO 80903, and **Michael J. Jacobson, Jr., Ning Shang, Shuo Shen** and **Andreas Stein**. *Explicit Formulas for Real Hyperelliptic Curves of Genus 2*.

The infrastructure on real hyperelliptic curves has been proposed for use in cryptographic protocols. Although the arithmetic of real curves is generally slower than imaginary curves, recent work has shown that some divisor additions can be replaced with faster baby steps. In order to make a fair comparison with protocols using imaginary curves, explicit formulas for divisor addition and doubling on real curves are needed. We present explicit formulas for genus 2 real hyperelliptic curves and compare the results with imaginary curves. (Received September 13, 2007)