1020-11-139 **Andreas Stein*** (astein@uwyo.edu), Department of Mathematics, University of Wyoming, 1000 East University Ave, Laramie, WY 82071-3036, and **Michael J Jacobson** and **Renate Scheidler**. *New Results on Real Hyperelliptic Curve Arithmetic.*

The generic model for arithmetic on hyperelliptic curve arithmetic is called the imaginary model. In this talk, we will discuss the so-called real model of a hyperelliptic curve. The details of the arithmetic is technically more involved, but turned out to be more flexible because of an additional much faster operation. Our main application of these ideas will be in cryptographic protocols based on hyperelliptic curve arithmetic. Using generic divisor arithmetic, the real model analogue of the Diffie-Hellman key exchange protocol is almost fifteen percent faster than conventional key exchange using imaginary hyperelliptic curves, with the most significant improvements occurring for low genus. This speed-up is established theoretically and confirmed numerically. The ideas of the improvements can be easily generalized to other cryptographic protocols where a similar speed-up can be obtained. These results exclude explicit formulas for low genus curves. Explicit formulas for genus two and three real hyperelliptic curves are currently developed and optimized. We remark that the same ideas lead to equivalent speed-ups in protocols based on the arithmetic in real quadratic number field arithmetic. (Received August 24, 2006)