1016-11-252 **Michael J Jacobson** and **Renate Scheidler*** (rscheidl@math.ucalgary.ca), Department of Mathematics and Statistics, University of Calgary, 2500 University Drive NW, Calgary, AB T2N 1N4, Canada, and **Andreas Stein**. *Real Hyperelliptic Curves, Part I: Theory and Algorithms.* Preliminary report.

Algebraic geometers and cryptographers are familiar with what we call for our purposes the "imaginary model" of a hyperelliptic curve. Another less familiar description of such a curve is the so-called "real model"; the terminology stems from the analogy to real and imaginary quadratic number fields. Structurally and arithmetically, the real model behaves quite differently from its imaginary counterpart. While divisor addition with subsequent reduction ("giant steps") is still essentially the same, the real representation no longer allows for unique representation of elements in the Jacobian by their reduced representatives. However, degree zero divisors in the real model exhibit a so-called infrastructure, with an additional, much faster operation ("baby steps"). We present the real model of a hyperelliptic curve and its two-fold baby step giant step divisor arithmetic. Part II of this talk will illustrate how to use these algorithms in the principal infrastructure for efficient cryptographic applications. (Received February 13, 2006)