RENATE SCHEIDLER, University of Calgary, Department of Mathematics & Statistics, 2500 University Drive NW, Calgary, Alberta, T2N 3Z4

Cryptography on Real Hyperelliptic Curves

Algebraic geometers and cryptographers are very familiar with what we like to call 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 model no longer allows for efficiently computable unique representation of elements in the Jacobian via reduced representatives. However, the real model exhibits 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. We also indicate how to use these algorithms for potential cryptographic and number theoretic applications.