SEBASTIEN LINDNER, Univerisity of Calgary
Divisor Arithmetic Over Low Genus Hyperelliptic Curves

Our main objective is to improve efficiency of low-genus hyperelliptic curve cryptosystems via alternative scalar multiplication algorithms and new explicit formulas. The basic operations in the divisor class group over a hyperelliptic curve are scalar multiplications, in other words adding a divisor to itself a fixed number of times. Divisor arithmetic on low-genus hyperelliptic curves is done by using explicit formulas described in terms of finite field operations. One way to increase efficiency is to use a double base algorithm for scalar multiplication where you represent the scalar as a sum of powers of two and three. The efficiency of using this algorithm over a single base algorithm becomes advantageous if you have fast explicit tripling formulas. We have produced explicit tripling formulas that are computationally faster than any other combination of doubling and adding, giving an increase in efficiency over all when using double base representation algorithms for scalar multiplication in the divisor class group.