1116-11-1455 **Michael J. Jacobson Jr.**, **Monireh Rezai Rad** and **Renate Scheidler*** (rscheidl@ucalgary.ca), Department of Mathematics and Statistics, 2500 University Drive NW, Calgary, Alberta T2N3Z4, Canada. *Comparison of scalar multiplication on real hyperelliptic curves.*

Real hyperelliptic curves admit two structures suitable for cryptography — the Jacobian (a finite abelian group) and the infrastructure (an "almost" abelian group). Mireles Morales described precisely the relationship between these two structures, and made the assertion that when implemented with balanced divisor arithmetic, the Jacobian generically yields more efficient arithmetic than the infrastructure for cryptographic applications. We confirm that this assertion holds for genus two curves, through rigorous analysis and the first detailed numerical performance comparisons, showing that cryptographic key agreement can be performed in the Jacobian without any extra operations beyond those required for basic scalar multiplication. However, for genus three curves, there is reason to believe that infrastructure scalar multiplication may slightly outperform scalar multiplication using balanced divisors; numerical experiments to that effect are currently work in progress as part of the second author's doctoral thesis. (Received September 19, 2015)