1023-11-1042 **Andreas Stein*** (astein@uwyo.edu), Department of Mathematics, University of Wyoming, 1000 E. University Ave., Laramie, WY 82071-3036, **Michael J Jacobson** (jacobs@cpsc.ucalgary.ca), Department of Computer Science, University of Calgary, 2500 University Drive NW, Calgary, Alberta T2N 1N4, Canada, and **Renate Scheidler** (rscheidl@math.ucalgary.ca), Department of Mathematics & Statistics, University of Calgary, 2500 University Drive NW, Calgary, Alberta T2N 1N4. *What is NUCOMP?* Preliminary report.

Here, we show how the theory and arithmetic of hyperelliptic curves presented in Renate Scheidler's talk can be employed for fast group operations on reduced divisors. We will explain the algorithm NUCOMP and how it works. In particular, we will analyze its complexity and provide evidence for its excellent performance. These considerations will have important applications to cryptographic protocols such as the Diffie-Hellman key exchange protocol or signature schemes based on hyperelliptic curve arithmetic. Even more general, the complexity analysis will show that NUCOMP is a faster way of computing the group operation or the infrastructure operation in any situation where hyperelliptic curve arithmetic is needed. It remains to be seen how explicit formulas for NUCOMP for low genus curves compare to the best known ones. (Received September 24, 2006)