1016-11-150 **Andreas Stein*** (astein@uwyo.edu), Department of Mathematics, University of Wyoming, 1000 E. University Ave., Laramie, WY 82071-3036, and **Michael John Jacobson** and **Renate Scheidler**. *Real Hyperelliptic Curves Part II: Algorithms and Application to Cryptography.*

Here, we show how the theory and arithmetic of real hyperelliptic curves presented in part I can be employed for fast scalar multiplication of reduced divisors and, more specifically, for an infrastructure version of the conventional Diffie-Hellman key exchange protocol. Using binary exponentiation techniques, an algorithmic analysis predicts our protocol to be approximately 15 percent faster than its imaginary counterpart. Numerical experiments confirm this expected speed-up, and the most significant improvement occurs for the cryptographically interesting case of low genus; the best results were in fact achieved for the case of a binary field of genus two. Time-permitting we will discuss analogous results for the key exchange protocol with real quadratic number fields. (Received February 09, 2006)