1056-12-2077 **Jason Worth Martin*** (martinjw@jmu.edu), MSC 1911 (305 Roop Hall), Harrisonburg, VA 22807. *Parallel Performance of Some SHA-3 Second Round Candidates.* Preliminary report.

The National Institute of Standards and Technology is currently holding the second round of a competition to select SHA-3, the next federal hashing standard. Fourteen candidate algorithms remain in the contest, and in this presentation we consider the parallel performance of several of the algorithms. We use two common parallel architectures: multi-core CPUs and video cards. Current video cards from NVIDIA have hundreds of processing cores which can be readily harnessed for data-parallel computations such as tree hashing. To create a fair comparison of the algorithms we place their compression functions inside of a single tree-based structure and investigate their performance on mid-range video cards and large multi-core systems when hashing extremely large messages. (Received September 23, 2009)