1046-08-1990 **Jason Worth Martin*** (martinjw@jmu.edu), MSC 1911 (Math Dept.), JMU, Harrisonburg, VA 22807. *ESSENCE: A Family of Cryptographic Hashing Algorithms.*

This paper describes the compression functions for a family of Merkle-Damgård based cryptographic hashing algorithms. The compression functions are based on a nonlinear, key-dependent permutation, E, of 256 or 512 bits built from 32 or 64 eight-bit nonlinear feedback shift-registers run in parallel with linear mixing between the shift-registers. The E permutation has been designed so that it can execute completely within the register file of modern 64-bit microprocessors and in constant time, thus increasing its resistance to side-channel attacks. We give a complete description of all criteria used for the constructions and provide differential and linear cryptanalysis. (Received September 16, 2008)