Single Core Implementation of Blue Midnight Wish Hash Function on VIRTEX 5 Platform

http://www.firstlight.cn 2010-11-09

This paper presents the design and analysis of an area efficient implementation of the SHA-3 candidate Blue MidnightWish hash function with different digest sizes of 256 and 512 bits on an FPGA platform. The core functionality with finalization implementation without padding stage of BMW on Xilinx Virtex-5 FPGA requires 51 slices for BMW- 256 and 105 slices for BMW-512. Both BMW versions require two blocks of memory: one memory block to store the intermediate values and hash constants and the other memory block to store the instruction controls. The proposed implementation achieves a throughput of 68.71 Mpbs for BMW-256 and 112.18 Mpbs for BMW-512.

存档文本