Abstract

Information is an asset in today’s life. Internet plays major role for sharing the information between two parties. To protect the information from attacks there exist several algorithms. Cryptographic hash functions are the one that is used for the purpose of modern security. In mobile computing, portables devices are used to share information. Most of portable devices are based on ARM processors. In this work, a BLAKE algorithm from SHA-3 finalists is selected for analysis on ARM Cortex A8 Processor. BLAKE is a hash function selected by NIST in SHA-3 competition. Many factors need to be considered such as utilization of memories ROM or RAM, power consumption and cycles required for particular algorithm. In this paper, the objective is to compare the performance of all variants of BLAKE in terms of cycles required on ARM Cortex A8.

References

SHA-3 Blake Finalist on Hardware Architecture of ARM Cortex A8 Processor


Index Terms

Computer Science
Circuits and Systems

Keywords
Cryptography, Hash functions, SHA-3, BLAKE, ARM11, ARM Cortex A8.