Abstract

Modified Grøstl - mGrøstl hash function was recently proposed by the authors as an alternative of one of the five finalist of SHA-3 competition namely Grøstl-256. This research paper presents the detailed analysis of algorithm along with performance evaluation of mGrøstl in eBASH project. According to the analysis, paper points out that different performance can be gained by adapting different platform.

References

Analysis of the Hash Function – Modified Grøstl

   - H. Wu, 2011, JH. Candidate to the NIST Hash Competition.

Index Terms

Computer Science

Keywords

Ebash Entropy Test Grøstl Hash Function Mgrøstl Sha3 Competition.