International Journal on Recent Researches In Science, Engineering & Technology
A Journal Established in early 2000 and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy.
It is an absolutely free (No processing charge No publishing charge etc) Journal Indexed in DIIF and SJIF.
Research Paper
Available online at: www.jrrset.com
Chief Editor : 1. Dr. M.Narayana Rao, Rtd. Professor, NIT, Trichy. (Engg.&Technology division)
2. Dr. N.Sandyarani, Ph.D., Professor, Chennai based Engg.College, (Science division)

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105
Volume 1, Issue 11, Nov. 2013
DIIF IF :1.46
SJIF IF: 1.329

SECURITY SURVEY OF SHA

A. Arul murugan

Abstract - Literature reported, several directions on the security of SHA - 256 . It has been shown that neither Dobbertins nor Chabaud and Jouxs attacks on MD-type hash functions seem to transpose to SSHA - 256 . Most features of the basic components of SHA - 256 provide a better security level than for preceding hash functions, even though the relative number of rounds may seem somewhat lower than for SHA - 1 for instance, and though the selection criteria and security arguments for design choices are difficult to reconstruct from the mere specification, in the absence of any public design report. Investigations on differential properties of the underlying compression function were made.