International Journal on Recent Researches In Science, Engineering & Technology

A Journal Established in early 2000 as National journal 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 charges, No publishing charges etc) Journal Indexed in DIIF and SJIF.

Research Paper

Available online at: www.jrrset.com

Chief Editors 1 : Dr. M.Narayana Rao, Ph.D., 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 2, Issue 4,
April 2014

DIIF IF :1.46
SJIF IF: 1.329

Security Analysis of the SHA - 2

A . SelvaKumar and S.Priya

Abstract - Literature reported several directions on the security of SHA-256 . We have shown that neither Dobertins nor Chabaud and Jouxs attacks on MD-type hash function seem to transpose to SHA-256 . Most features of basic components of SHA-256 provide a better security level than for preceding hash functions, even though the relative number of rounds may seem some what lower than for SHA-1 for instance ,and though the selection criteria and security arguments for some design choices are difficult to reconstruct from the mere specification , in the absence of any public design report . We have investigated differential properties of the underlying compression function and did not find any highly probable integrative characteristics, nor characteristics which extend to all rounds of the compression function. Finally, we have shown that a simplified version of SHA-256 where the round constraints are half-wise symmetric is not secure . In light of these observations, We conclude that non of the currently known attack methods can be successfully applied to SHA-256, and that we are not aware of any attack allowing to reduce the complexity of preimage or second preimage computations on SHA-256 to substantially less than 2256 or the complexity for collision and pseudo-collision search on SHA-256 to substantially less than the natural birthday collision bound which is 2 = 2 .