Cryptology ePrint Archive: Report 2013/150

Practical (Second) Preimage Attacks on TCS_SHA-3

Gautham Sekar and Soumyadeep Bhattacharya

Abstract: TCS_SHA-3 is a family of four cryptographic hash functions that are covered by an US patent (US 2009/0262925). The digest sizes are 224, 256, 384 and 512 bits. The hash functions use bijective functions in place of the standard, compression functions. In this paper we describe first and second preimage attacks on the full hash functions. The second preimage attack requires negligible time and the first preimage attack requires $O(2^{36})$ time. In addition to these attacks, we also present a negligible-time second preimage attack on a strengthened variant of the TCS_SHA-3. All the attacks have negligible memory requirements.

Category / Keywords: secret-key cryptography / Cryptanalysis, hash function, (second) preimage attack

Date: received 13 Mar 2013, last revised 15 Mar 2013

Contact author: sgautham at isichennai res in

Available formats: Postscript (PS) | Compressed Postscript (PS.GZ) | PDF | BibTeX Citation

Version: 20130315:110604 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]