Cryptology ePrint Archive: Report 2011/565

Cryptographic Hash Functions: Recent Design Trends and Security Notions

Saif Al-Kuwari and James H. Davenport and Russell J. Bradford

Abstract: Recent years have witnessed an exceptional research interest in cryptographic hash functions, especially after the popular attacks against MD5 and SHA-1 in 2005. In 2007, the U.S. National Institute of Standards and Technology (NIST) has also significantly boosted this interest by announcing a public competition to select the next hash function standard, to be named SHA-3. Not surprisingly, the hash function literature has since been rapidly growing in an extremely fast pace. In this paper, we provide a comprehensive, up-to-date discussion of the current state of the art of cryptographic hash functions security and design. We first discuss the various hash functions security properties and notions, then proceed to give an overview of how (and why) hash functions evolved over the years giving raise to the current diverse hash functions design approaches.

Category / Keywords: Hash Functions, Design, Compression Function, Security Notions, Survey

Publication Info: In Short Paper Proceedings of Inscrypt '10

Date: received 19 Oct 2011, last revised 6 Jan 2012

Contact author: s alkuwari at bath edu