Sedov, G. K.

Summary: In January 2013 the National standard of the Russian Federation GOST R 34.11-94 defining the algorithm and computational procedure for hash function was replaced by GOST R 34.11-2012. A family of hash functions Streebog was approved as a new standard. We analyse the family Streebog from the mathematical cryptography viewpoint and prove that it is secure against preimage and collision attacks.

MSC:
94A60 Cryptography
68P25 Data encryption (aspects in computer science)
11T71 Algebraic coding theory; cryptography (number-theoretic aspects)

Keywords:
hash functions; mathematical cryptography; streebog; GOST R 34.11-2012

Full Text: DOI MNR

References:
[6] Stam M., Blockcipher based hashing revisited, IACR Cryptology ePrint Archive,
[8] AlTawy R., Yousef A. M., Watch your constants: malicious Streebog, IACR Cryptology ePrint Archive,
[9] Ma B., Li B., Hao R., Li X., Improved cryptanalysis on reduced-round GOST and Whirlpool hash function (Full version), IACR Cryptology ePrint Archive, - Zbl 1314.94088

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.