Sedov, G. K.

The security of GOST R 34.11-2012 against preimage and collision attacks. (Russian. English summary) Zbl 1475.94163

Mat. Vopr. Kriptografii 6, No. 2, 79-98 (2015).

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:

[1] GOST R 34.11-2012, Natsionalnyi standart Rossiiskoi Federatsii. Informatsionnaya tekhnologiya. Kriptograficheskaya zaschita informatsii. Funktsiya kheshirovaniya, Standartinform, Moskva, 2012

[2] Mendel F., Pramstaller N., Rechberger C., Kontak M., Szmidt J., "Cryptanalysis of the GOST hash function", CRYPTO'2008, Lect. Notes Comput. Sci., 5157, 2008, 162-178 · Zbl 1183.94042

[3] AlTawy R., Kircanski A., Youssef A. M., Rebound attacks on Stribog, IACR Cryptology ePrint Archive, · Zbl 1368.94081

[4] Wang Z., Yu H., Wang X., Cryptanalysis of GOST R hash function, IACR Cryptology ePrint Archive, · Zbl 1358.94083

[5] Dodis Y., Ristenpart T., Shrimpton T., Salvaging Merkle-Damg?ard for practical applications, IACR Cryptology ePrint Archive, · Zbl 1239.94047

[6] Stam M., Blockcipher based hashing revisited, IACR Cryptology ePrint Archive,

[7] AlTawy R., Youssef A. M., Preimage attacks on reduced-round Stribog, IACR Cryptology ePrint Archive, · Zbl 1288.94048

[8] AlTawy R., Youssef 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