Saarinen, M.-J. O.

StriBob: authenticated encryption from GOST R 34.11-2012 LPS permutation. (English)

Zbl 1475.94157
Mat. Vopr. Kriptografii 6, No. 2, 67-78 (2015).

Summary: Authenticated encryption algorithms protect both the confidentiality and integrity of messages in a single processing pass. We show how to utilize the $L \circ P \circ S$ transform of the Russian GOST R 34.11-2012 standard hash "Streebog" to construct an efficient, lightweight algorithm for Authenticated Encryption with Associated Data (AEAD) via the Sponge scheme. The proposed algorithm "StriBob" has attractive security properties, is faster than the Streebog hash alone, twice as fast as the GOST 28147-89 encryption algorithm, and requires only a modest amount of running-time memory. StriBob is a Round 1 candidate in the CAESAR competition.

MSC:

94A60 Cryptography
94A62 Authentication, digital signatures and secret sharing

Keywords:

StriBob; authenticated encryption; GOST R 34.11-2012; streebog; sponge construction; duplexwrap; MonkeyDuplex; CAESAR

Software:

Keccak; Whirlpool

Full Text: DOI MNR

References:

[1] Andreeva E., Mennink B., Preneel B., Security reductions of the second round SHA-3 candidates, IACR ePrint, · Zbl 1371.94619

[2] Barreto P. S. L. M., Rijmen V., The Whirlpool hashing function. NESSIE Algorithm Specification,

[3] Bertoni G., Daemen J., Peeters M., Assche G. V., "Duplexing the sponge: Singlepass authenticated encryption and other applications", SAC 2011, Lect. Notes Comput. Sci., 7118, 2011, 320-337 · Zbl 1292.94030

[4] Bertoni G., Daemen J., Peeters M., Assche G. V., The Keccak reference, version 3.0, NIST SHA3 Submission Document, January 2011

[5] Bertoni G., Daemen J., Peeters M., Assche G. V., "Permutation-based encryption, authentication and authenticated encryption", DIAC 2012, 2012 · Zbl 1292.94030

[6] Bertoni G., Daemen J., Peeters M., Assche G. V., Keer R. V., CAESAR submission: Keyak v1,

[7] Biham E., Dunkelman O., A framework for iterative hash functions - HAIFA, IACR ePrint, · Zbl 06015144

[8] Biham E., Shamir A., Differential cryptanalysis of the Data Encryption Standard, Springer, 1993 · Zbl 0778.94005

[9] Chang S., Perlner R., Burr W. E., Turan M. S., Kelsey J. M., Paul S., Bassham L. E., Third-round report of the SHA-3 cryptographic hash algorithm competition, Tech. Rep. NISTIR 7896, Nat. Inst. Stand. Technol., November, 2012

[10] Daemen J., Rijmen V., The design of Rijndael: AES - the Advanced Encryption Standard, Springer, 2002 · Zbl 1065.94005

[11] Damgård I., "A design principle for hash functions", Lect. Notes Comput. Sci., 435, 1989, 416-427

[12] Dolmatov V., Degtyarev A., GOST R 34.11-2012: Hash Function, ITEF RFC 6986, August 2013

[13] GOST. Cryptographic protection for data processing system. GOST 28147-89, 1989 (in Russian)

[14] GOST. Cryptographic protection of information, hash function. GOST R 34.11-94, 1994 (in Russian)

[15] GOST. Information technology. Cryptographic protection of information, hash function. GOST R 34.11-2012, 2012 (in Russian)

[16] Kazymyrov O., Kazymyrova V., "Algebraic aspects of the Russian hash standard GOST R 34.11-2012", CTCrypt'13 (June 23-24, 2013, Ekaterinburg, Russia), 2013; IACR ePrint,

[17] Knudsen L.,Wagner D., "Integral cryptanalysis (extended abstract)", FSE 2002, Lect. Notes Comput. Sci., 2365, Springer, 2002, 112-127 · Zbl 1045.94527

[18] Lamberger M., Mendel F., Rechberger C., Rijmen V., Schläffer M., "Rebound distinguishers: Results on the full whirlpool compression function", ASIACRYPT'09, Lect. Notes Comput. Sci., 5912, ed. Matsui M., 2009, 126-143 · Zbl 1267.94079

[19] Lamberger M., Mendel F., Schläffer M., Rechberger C., Rijmen V., "The rebound attack and subspace distinguishers: Application to Whirlpool", J. Cryptology, 28:2 (2015), 257-296 · Zbl 1314.94082 · doi:10.1007/s00145-013-9166-5

[20] Matsui M., "Linear cryptoanalysis method for DES cipher", EUROCRYPT'93, Lect. Notes Comput. Sci., 765, ed. Helleseth T., 1994, 386-397 · Zbl 0951.94519

[21] Matyas S., Meyer C., Ossas J., "Generating strong one-way functions with cryptographic algorithm", IBM Technical Disclosure Bulletin, 27 (1985), 5658-5659

[22] Mendel F., Pramstaller N., Rechberger C., Kontak M., Szmidt J., "Cryptanalysis of the GOST hash function", CRYPTO 2008, Lect. Notes Comput. Sci., 5157, 2008, 162-128 · Zbl 1183.94042

[23] Merkle R., Secrecy, Authenticatication, and public key systems, PhD thesis, Stanford University, 1979

[24] Advanced Encryption Standard (AES), FIPS 197, NIST, 2001

[25] The keyed-hash message authentication code (HMAC), FIPS 198-1, NIST, July 2008

[26] Bernstein D., CAESAR call for submissions,

[27] Saarinen M.-J. O., "Beyond modes: Building a secure record protocol from a cryptographic sponge permutation", CT-RSA 2014, Lect. Notes Comput. Sci., 8366, 2014, 270-285 · Zbl 1337.94067

[28] Saarinen M.-J. O., The STRIBOBr1 authenticated encryption algorithm, CAESAR, 1st Round,