Nesterenko, A. Yu.

On a family of universal hash functions. (Russian. English summary) Zbl 1472.68052

Mat. Vopr. Kriptografii 6, No. 3, 135-151 (2015).

Summary: We construct a new family of compressing mappings by means of superposition of several bijective mappings and mappings with specified properties. All functions in this family are proved to be universal hash functions. Concrete examples of functions from the family which are suitable for cryptographic applications are supplied.

MSC:

68P25 Data encryption (aspects in computer science)
94A60 Cryptography

Keywords:

compressing mappings; universal hash functions

Software:

MMH

Full Text: DOI MNR

References:

[1] Alferov A. P., Zubov A. Yu., Kuzmin A. S., Cheremushkin A. V., Osnovy kriptografii, Uchebnoe posobie, Gelios ARV, M., 2001, 480 pp.

[2] Ilyasov I. I., "K raspredeleniyu prostykh chisel v mnogochlenakh vtoroi stepeni s tselymi koeffitsientami", Chebyshevskii sbornik, 14:1 (2013), 56-60

[3] Lebedev P. A., Nesterenko A. Yu., "Rezhim shifrovaniya s vozmozhnostyu autentifikatsii", Sistemy vysokoi dostupnosti, 9:3 (2013), 6-13

[4] Nesterenko Yu. V., Teoriya chisel, Akademiya, M., 2008, 272 pp.

[5] Serpinskii V., O reshenii uravnenii v tselykh chislakh, Izd-vo fiz.-mat. lit., M., 1961, 88 pp.

[6] B. A. Pogorelov, V. N. Sachkov (red.), Slovar kriptograficheskikh terminov, MTsMNO, M., 2006, 94 pp.

[7] Bellare M., Canetti R., Krawczyk H., "HMAC: Keyed-hashing for message authentication", Internet Engineering Task Force, Request for Comments (RFC) 2104, February 1997

[8] Black J., Halevi S., Krawczyk H., Krovetz T., Rogaway P., "UMAC: Fast and secure message authentication", CRYPTO' 99, Lect. Notes Comput. Sci., 1666, 1999, 216-233 · Zbl 0940.94020 · doi:10.1007/3-540-48405-1$_1$4

[9] Black J., Rogaway P., "CBC MACs for arbitrary-length messages: The three-key constructions", CRYPTO 2000, Lect. Notes Comput. Sci., 1880, 2000, 197-215 · Zbl 0995.94545 · doi:10.1007/3-540-44598-6$_1$2

[10] Boesgaard M., Scavenius O., Pedersen T., Christensen T., Zenner E., "Badger – a fast and provably secure MAC", Appl. cryptogr. network secur. 3rd Int. Conf., ACNS 2005, Lect. Notes Comput. Sci., 3531, 2005, 176-191 · Zbl 1126.68384 · doi:10.1007/11496137$_1$3

[11] Carter J. L., Wegman M. N., "Universal classes of hash functions", J. Comput. Syst. Sci., 18 (1979), 143-154 · Zbl 0412.68090 · doi:10.1016/0022-0000(79)90044-8

[12] Etzel M., Patel S., Ramzan Z., "Square Hash: Fast message authentication via optimized universal hash functions", CRYPTO' 99, Lect. Notes Comput. Sci., 1666, 1999, 234-251 · Zbl 0940.94021 · doi:10.1007/3-540-48405-1$_1$5

[13] FIPS PUB 198-1. Computer Security. Cryptography. The Keyed-Hash Message Authentication Code (HMAC), 2008, 13 pp.

[14] Halevi S., Krawczyk H., "MMH: software message authentication in the Gbit/second rates", FSE' 97, Lect. Notes Comput. Sci., 1267, 1997, 172-189 · Zbl 1385.94039 · doi:10.1007/BFb0052345

[15] Handschuh H., Preneel B., "Key-recovery attacks on universal hash function based MAC algorithms", CRYPTO 2008, Lect. Notes Comput. Sci., 5157, 2008, 144-161 · Zbl 1183.94035 · doi:10.1007/978-3-540-85174-5$_9$

[16] Iwata T., Kurosawa K., "OMAC: One-key CBC MAC", FSE 2003, Lect. Notes Comput. Sci., 2887, 2003, 129-153 · Zbl 1254.94033 · doi:10.1007/978-3-540-39887-5$_1$1

[17] Krovetz T., "Message authentication on 64-bit architectures", SAC 2006, Lect. Notes Comput. Sci., 4356, 2007, 327-341 · Zbl 1161.68444 · doi:10.1007/978-3-540-74462-7$_2$3

[18] Nandi M., On the minimum number of multiplications necessary for universal hash constructions, IACR Cryptology ePrint Archive, № 574, 2013

[19] Preneel B., Analysis and design of cryptographic hash functions, Doct. diss., Katholieke Univ. Leuven, 1993

[20] Stinson D. R., "Universal hashing and authentication codes", CRYPTO 91, 1991, 74-85 · Zbl 0789.68050

[21] Stinson D. R., "Universal hashing and message authentication codes", Des., Codes and Cryptogr., 4:4 (1994), 369-380 · Zbl 0812.94011 · doi:10.1007/BF01388651

[22] Wegman M. N., Carter J. L., "New hash functions and their use in authentication and set equality", J. Comput. Syst. Sci., 22:3 (1981), 265-279 · Zbl 0461.68074 · doi:10.1016/0022-0000(81)90033-7