МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2017 Т. 8 № 2 С. 117–130

УДК 519.719.2

A new authenticated encryption mode for arbitrary block cipher based on universal hash function

A. Yu. Nesterenko

National Research University Higher School of Economics, Moscow

Получено 18.III.2016

Abstract. In this article we present a new authenticated encryption mode for arbitrary block cipher. This mode is a combination of well known XEX (Xor-Encryption-Xor) mechanism used in XTS encryption mode and universal hash function with predetermined properties from special class of functions. The bit length of authentication code being twice as much as the length of a cipher block is an important feature of our mode. The other important feature is the possibility of parallel implementation. The description, some security considerations and aspects of practical implementation are supplied.

Keywords: authenticated encryption, block cipher, universal hash function

Новый режим аутентифицированного шифрования для произвольного блочного шифра на основе универсальной функции хэширования

А. Ю. Нестеренко

Национальный исследовательский университет «Высшая школа экономики», Москва

Аннотация. В работе предлагается новый режим аутентифицированного шифрования, который является комбинацией хорошо известного режима XEX (Xor-Encryption-Xor) и универсальной функции хэширования с заданными свойствами из специального класса. Важной особенностью данного режима является тот факт, что длина кода аутентификации в два раза превосходит длину входного блока используемого шифра. Другой важной особенностью является возможность распараллеливания. В работе приводятся описание режима, обоснование его безопасности и рассматриваются вопросы практической реализации.

Ключевые слова: аутентифицированное шифрование, блочный шифр, универсальная функция хэширования

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 2, pp. 117–130 (Russian)

References

[1] Black J., Halevi S., Krawczyk H., Krovetz T., Rogaway P., "UMAC: Fast and provably secure message authentication". In: *"CRYPTO '99*", Lect. Notes Comput. Sci., **1666**, 1999, 216–233.

[2] Boesgaard M., Scavenius O., Pedersen T., Christensen T., Zenner E., "Badger — a fast and provably secure MAC". In: *"Appl. Crypt. Network Secur., ACNS 2005*", Lect. Notes Comput. Sci., **3531**, 2005, 176–191.

[3] Carter L., Wegman M., "Universal classes of hash functions", *J. Comput. Syst. Sci.*, **18**:2 (1979), 143–154.

[4] *FIPS-197. Announcing the Advanced Encryption Standard (AES)*: NIST, 2001, 47 pp.

[5] *GMPLIB. The GNU Multiple Precision Arithmetic Library*, 2016, https://gmplib.org/.

[6] *GOST R 34.12–2015. Information technology. Cryptographic data security. Block ciphers*, Moscow: Standardinform, 2015 (in Russian).

[7] *GOST R 34.13–2015. Information technology. Cryptographic data security. Modes of operation for block ciphers*, Moscow: Standardinform, 2015 (in Russian).

[8] *IEEE Std 1619-2007, The XTS-AES Tweakable Block Cipher*: Inst. Electr. Electron. Eng., Inc., 2008.

[9] Lebedev P. A., Nesterenko A. Yu., "Authenticated encryption mode", *Systemy vysokoi dostupnosti*, **9**:3 (2013), 6–13 (in Russian).

[10] Lyskov M., Rivest R., Wagner D., "Tweakable Block Ciphers", *J. Cryptol.*, **24** (2011), 588–613.

[11] McGrew D., Viega J., "The security and performance of the Galois/Counter Mode (GCM) of operation". In: "*INDOCRYPT 2004*", Lect. Notes Comput. Sci., **3348**, 343-355.

[12] Nandi M., *FSE 2014*, Lect. Notes Comput. Sci., **8540**, 2014.

[13] Nesterenko A. Yu., "On a family of universal hash functions", *Mathematical Aspects of Cryptography*, **6**:3 (2015), 135–151 (in Russian).

[14] *NIST Special Publication 800-38A. Recommendation for Block Cipher Modes of Operation*, 2001, http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf.

[15] *NIST Special Publication 800-38E. Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices*, 2010, http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf.

[16] *Addendum to NIST Special Publication 800-38A. Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode*, 2010, http://csrc.nist.gov/publications/nistpubs/800-38a/addendum-to-nist-sp800-38A.pdf.

[17] Preneel B., *Analysis and Design of Cryptographic Hash Functions.*, Leuven: Katholieke Univ. Leuven, 1993.

[18] Rogaway P., "Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC". In: *"ASIACRYPT 2004*", Lect. Notes Comput. Sci., **3329**, 2004, 16-31.

[19] Saarinen M.-J. O., "Cycling attacks on GCM, GHASH and other polynomial MACs and hashes". In: "*FSE 2012*", Lect. Notes Comput. Sci., **7549**, 2012, 216–225.

[20] Saarinen M.-J. O., *The implemetation of Russian GOST R 34/12-2015 cipher "Kuznetchik"*, 2015, https://github.com/mjosaarinen/kuznechik.

[21] 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.