МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2017 Т. 8 № 2 С. 39–50

УДК 519.719.2

On the properties of the CTR encryption mode of Magma and Kuznyechik block ciphers with re-keying method based on CryptoPro Key Meshing

L. R. Ahmetzyanova, E. K. Alekseev, I. B. Oshkin, S. V. Smyshlyaev, L. A. Sonina

CryptoPro LLC, Moscow

Получено 03.IV.2016

Abstract. Security bounds for the Magma cipher CTR encryption mode with the CryptoPro Key Meshing (CPKM) re-keying method are obtained for the standard security model and side channel information model. A modified re-keying method better than CPKM is proposed. Operational features of the Kuznyechik cipher CTR encryption mode for several re-keying methods are discussed.

The work was supported by the Russian Foundation of Basic Research, the project 16-01-00226 A.

Keywords: provable security, encryption mode, block cipher, GOST, re-keying

О свойствах блочных алгоритмов шифрования Магма и Кузнечик в режиме CTR с преобразованием ключа методом CryptoPro Key Meshing

Л. Р. Ахметзянова, Е. К. Алексеев, И. Б. Ошкин, С. В. Смышляев, Л. А. Сонина

ООО «Крипто-Про», Москва

Аннотация. Для шифра Магма с преобразованием ключа методом CryptoPro Key Meshing (CPKM) получены оценки стойкости в рамках стандартной модели и модели с информацией из побочных каналов. Предложена модификация алгоритма преобразования ключа, улучшенная по сравнению с CPKM. Обсуждаются эксплуатационные характеристики шифра Кузнечик в режиме CTR для нескольких методов преобразования ключа.

Работа выполнена при поддержке РФФИ, проект 16-01-00226 А.

Ключевые слова: доказуемая стойкость, режим шифрования, блочный шифр, ГОСТ, смена ключа

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 2, pp. 39–50 (Russian)

References

[1] *GOST R 34.12-2015. Information technology. Cryptographic protection of information. Block ciphers*, Moscow: Standartinform, 2015 (in Russian).

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

[3] Bellare M., Desai A., Jokipii E., Rogaway P., "A concrete security treatment of symmetric encryption". In: "*Proc. 38th Ann. Symp. Found. Comput. Sci.* (FOCS '97)": IEEE, 1997, 394–403.

[4] Popov V., Kurepkin I., Leontiev S., "Additional cryptographic algorithms for use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 algorithms". In: "*IETF RFC 4357*", 2006.

[5] Mironkin V., "On some probabilistic characteristics of the "CryptoPro Key Meshing" method", *Problemy Inform. Bezopasnosti. Komp'uternye systemy*, № 4 (2015) (In Russian).

[6] Matsui M., "Linear cryptanalysis method for DES cipher". In: "*EUROCRYPT'93*", Lect. Notes Comput. Sci., **765**, 1994, 386–397.

[7] Biham E., Shamir A., "Differential cryptanalysis of DES-like cryptosystems". In: "*CRYPTO'90*", Lect. Notes Comput. Sci., **537**, 1990, 2–21.

[8] *GOST 28147-89. Cryptographic Protection for Data Processing System, Gosudarstvennyi Standard of USSR*: Government Committee of the USSR for Standards, 1989 (In Russian).

[9] Ahmetzyanova L. R., Alekseev E. K., Oshkin I. B., Smyshlyaev S. V., Sonina L. A., *On the properties of the CTR encryption mode of the Magma and Kuznyechik block ciphers with re-keying method based on CryptoPro Key Meshing*, Cryptology ePrint Archive, Report 2016/628, http://eprint.iacr.org/2016/628.