МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2017 Т. 8 № 2 С. 51 – 64

УДК 519.719.2

The influence of linear mapping reducibility on the choice of round constants

D. A. Burov [1], **B. A. Pogorelov** [2]

[1] TVP Laboratories, Moscow
[2] Academy of Cryptography of the Russian Federation, Moscow

Получено 19.III.2016

Abstract. The influence of reducibility of linear mappings on the security of block ciphers is studied. It is shown that the replacement of only two key schedule constants of Khazad block cipher leads to the appearance of weak key classes. We study invariant subspaces of the Kuznyechik linear mapping and demonstrate that there are no weak key schedule constants similar to Khazad. But the choice of other linear mappings constructed similarly to the original Kuznyechik mapping and choice of other constants may results in the appearance of weak keys.

Keywords: block cipher, Kuznyechik, Khazad, invariant subspace, reducible linear mapping, key schedule constants

Влияние приводимости линейного преобразования на выбор раундовых констант

Д. А. Буров [1], **Б. А. Погорелов** [2]

[1] *Лаборатории ТВП, Москва*
[2] *Академия криптографии Российской Федерации, Москва*

Аннотация. Исследуется влияние приводимости линейного преобразования на стойкость блочных шифрсистем. Показано, что при замене двух констант в алгоритме развертывания ключа шифра Khazad возникают классы слабых ключей. Изучаются также инвариантные подпространства линейного преобразования шифра Кузнечик; показано, что в отличие от шифра Khazad для него не существует слабых констант алгоритма развертывания ключа. Выбор другого линейного преобразования, аналогичного используемому в шифре Кузнечик, и других констант алгоритма развертывания ключа ключа может привести к появлению слабых ключей.

Ключевые слова: блочный шифр, Кузнечик, Khazad, инвариантное подпространство, приводимое линейное преобразование, константы, алгоритм развертывания ключа

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 2, pp. 51–64 (Russian)

References

[1] Barreto P., Rijmen V., "The Khazad Legacy-Level Block Cipher". In: "*First Open NESSIE Workshop. Submission to NESSIE*", 2000.

[2] Bulygin S., Walter M., "Study of the invariant coset attack on PRINT cipher: more weak keys with practical key recovery", Cryptology ePrint Archive. Report 2012/085.

[3] Burov D. A., Pogorelov B. A., "An attack on 6 rounds of Khazad", *Mathematical Aspects of Cryptography*, **2**:7 (2016), 35–46.

[4] Daemen J., *Cipher and hash function design strategies based on linear and differential cryptanalysis*, Leuven, Belgium: K. U. Leuven, 1995, 252 pp.

[5] *D.STVL.9. Ongoing Research Areas in Symmetric Cryptography*, 2008 IST-2002-507932. ECRYPT. European Network of Excellence in Cryptology.

[6] Guo J., Jean J., Nicolic I., Qiao K., Sasaki Y., Meng Sim S., "Invariant subspace attack against full Midory64", Cryptology ePrint Archive. Report 2015/1189.

[7] Leander G., Abdelraheem M., Alkhzaimi H., Zenner E., "A cryptanalysis of PRINT cipher: The invariant subspace attack". In: "*CRYPTO'11*", Lect. Notes Comput. Sci., **6841**, 2011, 206–221.

[8] Leander G., Minaud B., Sonjom S., "A generic approach to invariant subspace attacks: cryptanalysis of Robin, iSCREAM and Zorro". In: "*EUROCRYPT'15*", Lect. Notes Comput. Sci., **9056**, 2015, 254–283.

[9] Pogorelov B. A., Pudovkina M. A., "On the distance from permutations to imprimitive groups for a fixed system of imprimitivity", *Discrete Math. Appl.*, **24**:2 (2014), 95–108.

[10] Pogorelov B. A., Pudovkina M. A., "Factor structures of transformations", *Mathematical Aspects of Cryptography*, **3**:3 (2012), 81–104 (in Russian).

[11] Pogorelov B. A., Pudovkina M. A., "Combinatorial characterization of XL-layers", *Mathematical Aspects of Cryptography*, **4**:3 (2013), 99–129 (in Russian).

[12] Shishkin V., Dygin D., Lavrikov I., Marshalko G., Rudskoy V., Trifonov D., "On a new Russian Encryption Standard", *Mathematical Aspects of Cryptography*, **6**:2 (2015), 29–34.