МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2017 Т. 8 № 1 С. 51–68

УДК 519.719.2

Analyzing the influence of linear redundancy in S-boxes on the affine equivalence within XSL-like round functions

Nguyen Bui Cuong, Nguyen Van Long, Hoang Dinh Linh

Institute of Cryptography Science and Technology, Government Information Security Committee, Viet Nam

Получено 10.VI.2016

Abstract. We show that S-boxes based on finite field inversion always possess complete linear redundancy. Next, we consider the influence of linear redundancy of S-boxes on the affine equivalence of component functions within XSL-like round functions in the general case. Then, we propose an effective practical approach to test this. Finally, some experimental results on the round functions within the Kuznyechik and AES are presented.

Keywords: Boolean functions, S-boxes, round function, block cipher, affine equivalence, linear redundancy

Анализ влияния линейной избыточности в S-боксах на аффинную эквивалентность в раундовых функциях XSL-схем

Нгуен Буй Куонг, Нгуен Ван Лонг, Хоанг Динь Линь

Институт криптографических наук и технологий, Государственный комитет защиты информации, Вьетнам

Аннотация. Показано, что S-боксы, основанные на операции обращения в конечном поле, всегда обладают полной линейной избыточностью. В общем случае рассматривается влияние линейной избыточности S-боксов на аффинную эквивалентность компонентных функций в раундовых функциях XSL-схем. Предлагается эффективный практический метод проверки наличия этих свойств. Приводятся экспериментальные результаты для раундовых функций в Кузнечике и AES.

Ключевые слова: булевы функции, S-боксы, раундовая функция, блочный шифр, аффинная эквивалентность, линейная избыточность

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 1, pp. 51–68 (Russian)

Список литературы

[1] Fuller J., Millan W., "Linear redundancy in S-boxes". In: "*Fast Software Encryption*", Lect. Notes Comput. Sci., **6061**, 2010, 73–80

[2] Daemen J., Rijmen V., *The Design of Rijndael: AES — The Advanced Encryption Standard*, Heidelberg etc.: Springer, 2002, xvii+238 p pp.

[3] Aoki K., Ichikawa T., Kanda M., Matsui M., Moriai S., Nakajima J., Tokita T., "Camellia: A 128-bit block cipher suitable for multiple platforms—design and analysis". In: "*Selected Areas in Cryptography*", Lect. Notes Comput. Sci., **2012**, 2001, 39–56.

[4] Rijmen V., Daemen J., Preneel B., Bosselaers A., De Win E., "The cipher SHARK". In: "*Fast Software Encryption*", Lect. Notes Comput. Sci., **1039**, 1996, 99–111.

[5] Ivanov G., Nikolov N., Nikova S., "Reversed genetic algorithms for generation of bijective S-boxes with good cryptographic properties", Cryptology ePrint Archive, Report 2014/801 (2014), http://eprint/iacr.org/2014/801.pdf.

[6] Youssef A. M., Tavares S. E., "Affine equivalence in the AES round function", *Discrete Appl.Math.*, **148**:2 (2005), 161–170.

[7] Lidl R., Niederreiter H., *Finite Fields. 2nd ed.*, Cambridge: Cambridge Univ. Press, 1997, xiv+755 p pp.

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

[9] *Information technology. Cryptographic Data Security. Block ciphers, GOST R 34.12-2015*, Federal Agency on Technical Regulating and Metrology, Moscow: Standardinform, 2015. (In Russian.)