УДК 681.3.06

О РАСПРОСТРАНЕНИИ КОНСТРУКЦИИ НИБЕРГ НА ПОЛЯ ГАЛУА НЕЧЕТНОЙ ХАРАКТЕРИСТИКИ

О. Н. ЖДАНОВ[1], А. В. СОКОЛОВ[2]

[1]*Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнёва, Россия, Красноярск, 660014, пр-т газеты «Красноярский Рабочий», 31*
[2]*Одесский национальный политехнический университет, Украина, Одесса, 65044, пр-т Шевченко 1*

Аннотация. Как известно, *S*-блоки конструкции Ниберг обладают криптографическими свойствами, ценными для практического применения. До настоящего времени эта конструкция рассматривалась только для полей характеристики 2. В данной статье конструкция Ниберг обобщена на поля нечетной характеристики. Введено понятие расстояния нелинейности *p*-функции, построен троичный аффинный код. Построены *S*-блоки подстановки конструкции Ниберг для характеристики поля $p = 3$ для всех длин $N \le 243$. Вычислены их расстояния нелинейности и показано, что они растут с ростом длины *S*-блока подстановки существенно быстрее в сравнении с полями характеристики $p = 2$.

АКТУАЛЬНОСТЬ ТЕМЫ

Одним из основных средств обеспечения конфиденциальности информации являются блочные симметричные криптографические алгоритмы. Стремительный рост вычислительной мощности ЭВМ обуславливает необходимость увеличения криптостойкости существующих алгоритмов, а также разработки новых. В этом направлении ведут работу многие исследователи и практики. Устойчивость алгоритма шифрования к наиболее распространенным видам криптоанализа определяется качеством блока замен — *S*-блока подстановки. В настоящее время уже считается общепринятым, что качество узлов замен характеризуется значениями нелинейности и лавинного эффекта [1, 2].

ПОДХОДЫ К ФОРМИРОВАНИЮ ТАБЛИЦ ЗАМЕН

Применительно к формированию таблиц замен можно выделить два основных подхода в разработке алгоритмов шифрования.

Примером первого подхода является признанный очень стойким алгоритм ГОСТ 28147-89 [2], который не определяет метода генерации блоков замен. Алгоритм подразумевает возможность использования различных методик построения блоков замен. Например в [3] предложена обоснованная методика поэтапного выбора булевых функций, являющихся компонентами блока замен, в которой учитываются не только значения нелинейности каждой из функций, составляющих блок, но и нелинейность всех возможных их нетривиальных линейных комбинаций. Отметим также, что при этом возможно одновременно решать задачу повышения устойчивости как к линейному, так и к дифференциальному криптоанализу, если использовать в качестве крите-

DOI: 10.20535/S0021347017120032

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Жданов, О. Н. *Методика выбора ключевой информации для алгоритма блочного шифрования*. М.: ИНФРА-М, 2013. 90 с.

2. Соколов, А. В. *Новые методы синтеза нелинейных преобразований современных шифров.* Germany: Lap Lambert Academic Pub., 2015. 100 с.

3. ГОСТ 28147-89. *Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования*. М.: ИПК Издательство стандартов, 1996. 28 с.

4. Mister, S.; Adams, C. Practical S-box design. *Proc. of Workshop in Selected Areas of Cryptography*, SAC'96, 1996. P. 61–76. URI: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.40.7715&rep=rep1&type=pdf.

5. Медведева, Т. Е. Оценка криптостойкости таблиц замен алгоритма ГОСТ 28147-89. *Решетневские чтения*, 2012. С. 666. URI: http://disk.sibsau.ru/website/reshetnevsite/materials/2012_2.pdf.

6. Чалкин, Т. А. Разработка методики выбора параметров для алгоритма построения узлов замен блочного шифра ГОСТ 28147-89. Актуальные проблемы безопасности информационных технологий: материалы III Международной научно-практической конференции / Под общей ред. О. Н. Жданова, В. В. Золотарева. Красноярск: Сиб. гос. аэрокосмич. ун-т, 2009. С. 33–38.

7. FIPS 197. [Electronic resource] Advanced encryption standard, 2001. URI: http://csrc.nist.gov/publications/.

8. Nyberg, K. Differentially uniform mappings for cryptography. *Advances in cryptology. Proc. of EUROCRYPT'93*, *Lecture Notes in Computer Science*, Vol. 765, P. 55–65, 1994. DOI: 10.1007/3-540-48285-7_6.

9. Мазурков, М. И.; Соколов, А. В. Нелинейные преобразования на основе полных клас сов изоморфных и автоморфных представлений поля GF(256). *Известия вузов. Радиоэлектроника*, Т. 56, № 11, С. 16–24, 2013. URI: http://radio.kpi.ua/article/view/S0021347013110022.

10. Мазурков, М. И.; Соколов, А. В. Криптографические свойства нелинейного преобразования шифра Rijndael на базе полных классов неприводимых полиномов. *Праці Одеського політехнічного університету*, № 2, С. 183–189, 2012. URI: http://pratsi.opu.ua/articles/show/864.

11. Амбросимов, А. С. Свойства бент-функций q-значной логики над конечными полями. *Дискрет. матем.*, Т. 6, № 3, С. 50–60, 1994. URI: http://mi.mathnet.ru/dm639.

12. Лидл, Р.; Нидеррайтер, Г. *Конечные поля*. М.: Мир, 1988. 808 с.

13. Kim, Y.-S.; Jang, J.-W.; No, J.-S.; Helleseth, T. On p-ary bent functions defined on finite fields. *Mathematical Properties of Sequences and Other Combinatorial Structures*. The Springer International Series in Engineering and Computer Science, vol. 726. Springer, Boston, MA, 2002, P. 65–76. DOI: 10.1007/978-1-4615-0304-0_8.

14. Zhdanov, O. N.; Sokolov, A. V. Block symmetric cryptographic algorithm based on principles of variable block length and many-valued logic. *Far East J. Electronics Commun.*, Vol. 16, No. 3, P. 573–589, 2016. DOI: 10.17654/EC016030573.

Поступила в редакцию 12.02.2015 После переработки 01.10.2017