УДК 681.3.06

О.Н.ЖДАНОВ[1], А.В.СОКОЛОВ[2]

О РАСПРОСТРАНЕНИИ КОНСТРУКЦИИ НИБЕРГ НА ПОЛЯ ГАЛУА НЕЧЕТНОЙ ХАРАКТЕРИСТИКИ

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

Аннотация. Как известно, S-блоки конструкции Ниберг обладают криптографическими свойствами, ценными для практического применения. До настоящего времени эта конструкция рассматривалась лишь 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 $p = 2$.

Abstract. As it is known, S-boxes of the Nyberg construction have the cryptographic properties, valuable for practical application. Up to the present time this construction has been considered only for fields of characteristic 2. In this paper, the Nyberg construction was generalized to fields of odd characteristic. The definition of the distance of non-linearity of the p-function is introduced, affine ternary code is built. Nyberg construction S-boxes for Galois field of characteristic $p = 3$ for all lengths $N \le 243$ are built. Their distance of nonlinearity is calculated and it is showed that it increase with increasing of S-box length significantly faster compared to fields of characteristic $p = 2$.

Ключевые слова: S-блок подстановки, конструкция Ниберг, трехзначная логика; S-box, Nyberg construction, three-valued logic.

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 критериев выбора и нелинейность, и динамическое расстояние [4…6]. Методика такого поэтапного выбора была программно реализована применительно к алгоритму ГОСТ 28147-89 в работе [1].

Наиболее характерным примером второго подхода может служить также считающийся стойким алгоритм Rijndael [7], в котором блок замен полностью определяется неприводимым полиномом над полем Галуа. В Rijndael использована конструкция Ниберг

[8], представляющая собой отображение в виде мультипликативно обратных элементов поля Галуа $GF(2^k)$

$$y = x^{-1} \bmod d[f(z), p], \quad y, x \in GF(2^k), \tag{1}$$

в комбинации с аффинным преобразованием

$$b = A \cdot y + a, \quad a, b \in GF(2^k), \tag{2}$$

где $f(z) = z^8 + z^4 + z^2 + z + 1$ — неприводимый над полем $GF(2^8)$ полином;

A — невырожденная матрица аффинного преобразования; a — вектор сдвига;

$p = 2$ — характеристика расширенного поля Галуа, $0^{-1} \equiv 0$ — по определению;

a, b, x, y — элементы расширенного поля Галуа $GF(2^k)$, которые рассматриваются как десятичные числа, либо двоичные векторы, либо полиномы степени $k-1$.

Среди показателей качества S-блоков наиболее часто выделяют следующие [2]:

– максимум из модулей элементов матрицы коэффициентов корреляции входных и выходных битов;

– количество нулей в матрице коэффициентов корреляции;

– нелинейность, понимаемая как расстояние до множества аффинных функций;

– алгебраическая степень нелинейности;

– период возврата подстановочной конструкции в исходное состояние.

Отметим, что S-блоки конструкции Ниберг обладают многими практически ценными криптографическими свойствами, такими как высокое расстояние нелинейности, равномерная минимизация коэффициентов корреляции, сравнительная простота технической реализации как с помощью табличного метода, так и с помощью операций над полями Галуа.

В работах [9…10] подробно исследованы нелинейные преобразования конструкции Ниберг на основе всех изоморфных и автоморфных представлений полей $GF(2^k)$ для $k \le 8$: представлены все неприводимые полиномы над полями, вычислены значения показателей качества определяемых этими полиномами S-блоков. Таким образом, полином из (1) является не единственным возможным для построения шифра. Возможность же выбора одного из множества неприводимых полиномов имеет практическое значение.

После публикации работ [9,10] появилась возможность объединить достоинства подходов ГОСТа и Rijndael.

Применение функций многозначной логики. В настоящее время активно развивается теория и практика применения многозначной логики [11] в вычислениях, в том числе и в криптографии. В частности, работы [12…13] посвящены проблемам синтеза нелинейных функций многозначной логики, которые применяются при построении S-блоков и генераторов псевдослучайных ключевых последовательностей. Работа [14] посвящена разработке и обоснованию криптографической стойкости блочного симметричного криптоалгоритма, функционирующего на основе принципов многозначной логики.

Актуальной является задача дальнейшего совершенствования методов синтеза S-блоков на основе функций многозначной логики. Как показали исследования, хорошей базой для построения S-блоков многозначной логики может послужить обобщенная на многозначный случай конструкция Ниберг.

Целью настоящей статьи является обобщение конструкции Ниберг на случай полей Галуа характеристики $p = 3$.

Определение 1 [11]. Функцией p-значной логики (далее p-функция) k переменных называется отображение $\{0,1,2,...,p-1\}^k \to \{0,1,2,...,p-1\}$. При $p=2$ получаем булевы функции.

Функция трехзначной логики (3-функция) — это отображение $\{0,1,2\}^k \to \{0,1,2\}$, т.е. правило, однозначно сопоставляющее вектору из k координат, принимающих значения 0,1,2 значение 0,1 или 2.

Так же, как и булевы функции, 3-функции можно задать аналитически, в виде вектора, в виде таблицы.

Определение 2 [2]. *Линейной* называется p-функция, аналитически задаваемая как

$$\varphi'(x_0,\ldots,x_{k-1}) = a_0x_0 + a_1x_1 + \ldots + a_{k-1}x_{k-1} (\mathrm{mod}\ p) = \sum_{i=0}^{k-1} a_i x_i (\mathrm{mod}\ p), \qquad (3)$$

где $a_0, a_1, ..., a_{k-1} \in \{0,1,...,p-1\}$.

Определение 3 [2]. *Аффинной* называется функция аналитического вида

$$\varphi(x_0,\ldots,x_{k-1}) = a_0x_0 + a_1x_1 + \ldots + a_{k-1}x_{k-1} + b(\mathrm{mod}\ p) = \sum_{i=0}^{k-1} a_i x_i + b(\mathrm{mod}\ p), \qquad (4)$$

где $a_0, a_1, ..., a_{k-1}, b \in \{0,1,...,p-1\}$. Как нетрудно заметить, единственным отличием общего аналитического вида аффинных функций от линейных является наличие свободного члена b, при этом если $b=0$, то функция вида (4) является линейной. Множество всех аффинных функций от n переменных обозначим A_k.

Например, для случая $k=3$ могут быть приведены все аффинные функции

$$A_3 = \begin{Bmatrix} 000000000 & 111111111 & 222222222 \\ 012012012 & 120120120 & 201201201 \\ 021021021 & 102102102 & 210210210 \\ 000111222 & 111222000 & 222000111 \\ 012120201 & 120201012 & 201012120 \\ 021102210 & 102210021 & 210021102 \\ 000222111 & 111000222 & 222111000 \\ 012201120 & 120012201 & 201120012 \\ 021210102 & 102021210 & 210102021 \end{Bmatrix}. \qquad (5)$$

В (5) каждая функция задана в виде вектора, состоящего из значений функции, приведенных в порядке возрастания аргумента, если его представить в виде чисел от 0 до 3^3-1.

По аналогии с двоичным случаем введем следующее определение.

Определение 4. Расстоянием между *p*-функциями будем называть сумму модулей разностей значений функций при одинаковых наборах значений переменных. Иными словами, это сумма модулей разностей соответствующих координат в векторном представлении.

Замечание. В случае $p=2$ мы получаем хорошо известное расстояние Хэмминга.

Пример. Пусть задана функция $g = x_0x_1$, тогда её векторное представление $g = (000012021)$. Найдем расстояние от этой функции до аффинных функций φ_0 и φ_1.

$$d(g,\varphi_0) = (000012021, 000000000) = 6, \quad d(g,\varphi_1) = (000012021, 012012012) = 5. \qquad (6)$$

Теперь мы можем определить *нелинейность* p-функции.

Определение 5. Расстоянием нелинейности p-функции назовем минимальное расстояние от этой функции до множества аффинных функций:

$$nl(f) = \min_{c \in A_k} d(f, c). \tag{7}$$

Соответственно, расстояние нелинейности S-блока подстановки определяется как минимум нелинейностей среди всех его компонентных p-функций $SNl = \min_i \{nl(\alpha_i)\}$.

Заметим, что нелинейность блока можно определить и иначе, а именно, как минимум из значений нелинейностей всех нетривиальных линейных комбинаций компонент блока, так сделано для $p = 2$ в монографии [1]. Предлагаемый здесь подход обеспечивает большую свободу в построении блока (большее количество возможных блоков) в сравнении с предложенным в [1].

Переход к полям характеристики 3. Рассмотрим поле $GF(3^k)$. Для построения конструкции Ниберг необходимо найти все неприводимые полиномы. Число этих полиномов определяется формулой [12, с.118]:

$$|W_k| = \frac{1}{k} \sum_{d \;\; \mathrm{k}} \mu(d) \cdot p^{(k/d)}\ , \tag{8}$$

где d — делители числа k, $\mu(d)$ — функция Мёбиуса, запись $d \;\; k$ означает, что d делит k.

В табл. 1 приведены мощности множеств неприводимых над полем $GF(3^k)$ полиномов в зависимости от k, вычисленные в соответствии с (8).

Таблица 1

k	2	3	4	5	6	7	8	9	10
$\lvert W_k \rvert$	3	8	18	48	116	312	810	2184	5880

Анализ данных табл. 1 приводит к задаче описания полных множеств неприводимых полиномов, которые могут быть использованы для построения S-блоков подстановки. Для решения данной задачи может быть использован алгоритм, приведенный в [9]. Например, полное множество неприводимых полиномов для $k = 2$:

$$x^2 + 1; \quad x^2 + x + 2; \quad x^2 + 2x + 2, \tag{9}$$

для $k = 3$:

$$\begin{gathered} x^3 + 2x + 1; \quad x^3 + 2x + 2; \quad x^3 + x^2 + 2; \\ x^3 + x^2 + x + 2; \quad x^3 + x^2 + 2x + 1; \quad x^3 + 2x^2 + 1; \\ x^3 + 2x^2 + x + 1; \quad x^3 + 2x^2 + 2x + 2. \end{gathered} \tag{10}$$

Для краткости множество неприводимых полиномов поля $GF(3^4)$ запишем в виде их десятичных эквивалентов:

$$\Upsilon_4 = \{86, 89, 92, 94, 97, 101, 110, 115, 118, 121, 125, 134, 137, 139, 145, 149, 151, 164\}. \tag{11}$$

Например, первому десятичному эквиваленту соответствует полином: $86_{10} = 10012_3 \to x^4 + x + 2$. Аналогичным образом выпишем множество полиномов пятой степени $k = 5$

$$\Upsilon_5 = \left\{ \begin{matrix} 250,251,257,265,274,275,281,287,289,295,307,311,314,317,319,322,326,329, \\ 331,334,337,341,355,367,373,374,379,386,389,391,397,398,406,409,413,425, \\ 428,430,437,445,446,458,461,466,469,470,478,482 \end{matrix} \right\}. \quad (12)$$

Для того, чтобы построить S-блок необходимо рассмотреть множество его входных значений в диапазоне от 0 до 242, которые представимы в виде десятичных эквивалентов, троичных векторов или полиномов. Для нахождения соответствующего элемента S-блока, находим элемент, обратный к данному элементу по модулю выбранного неприводимого полинома, проводя все вычисления по модулю 3, подобно (1)

$$y = x^{-1} \operatorname{modd}[\psi(x), p], \quad y, x \in GF(3^k) \quad (13)$$

где $\psi(x)$ — неприводимый полином из множества (12).

Переходя от полиномиального вида векторов y к троичному числу, записываем получившиеся числа в таблицу, теперь столбец младших цифр — это компонентная троичная функций α_0, следующий столбец — компонентная троичная функция α_1 и т.д.

Приведем пример S-блока, построенного в соответствии с (12) для неприводимого полинома $\psi(x) = x^5 + x^4 + x^2 + 2x + 2$ в поле $GF(3^5)$

$$\left[\begin{matrix} 0,1,2,113,170,199,223,155,85,179,42,79,195,129,30,98,145,172,103,41,75,184, \\ 101,209,138,60,231,189,206,94,14,139,233,127,132,219,65,163,174,43,178,19, \\ 10,39,102,162,72,175,161,151,215,89,193,242,135,188,157,227,114,228,25,130, \\ 197,81,107,36,166,121,143,202,148,212,46,105,83,20,177,78,77,11,104,63,176, \\ 74,198,8,111,141,120,51,218,236,125,156,29,136,207,100,15,146,97,22,44,18,80, \\ 73,164,64,235,180,123,86,154,3,58,133,126,124,182,216,88,67,194,110,117,92, \\ 116,33,229,13,61,140,34,115,226,54,95,205,24,31,131,87,241,68,183,16,99,160,70, \\ 152,201,49,149,168,112,7,93,56,190,210,147,48,45,37,106,192,66,240,153,222,4, \\ 208,17,185,38,47,82,76,40,9,109,238,118,144,21,173,204,191,55,27,158,187,165, \\ 52,122,12,232,62,84,5,224,150,69,213,186,137,28,96,171,23,159,214,71,203,211, \\ 50,119,237,90,35,225,230,169,6,200,220,134,57,59,128,221,26,196,32,239,108, \\ 91,217,181,234,167,142,53 \end{matrix} \right]. \quad (14)$$

Нулевая компонентная троичная функция данного S-блока подстановки имеет вид

$$\alpha_0 = \left\{ \begin{matrix} 00012221120021011210021210222101211202202000120211212212121 20 \\ 12110211212011020001020201110221101210110000020221110011122 10 \\ 21111020010120120011202011012012101022100012021202020010001 21 \\ 10222001220102010210221012012022012102220221001202021122221 0 \end{matrix} \right\}. \quad (15)$$

Расстояние нелинейности 3-функции (15) в соответствии с (7) равно $nl(\alpha_0) = 162$. Проведенные эмпирические исследования позволили установить, что расстояние нелинейности всех остальных компонентных булевых функций также равно $nl(\alpha_i) = 162, i = 0,1,...,4$, а, соответственно, $Snl = 162$, причем расстояние нелинейности сохраняет свое значение для любого вида используемого неприводимого полинома (12).

Численное значение нелинейности S-блоков подстановки длины $N = 3^k$ или $N = 2^m$ конструкции Ниберг над полями $GF(3^k)$ для значений $k = 2,3,...,5$ и над полями $GF(2^m)$ для значений $m = 2,3,...,8$ приведены в виде соответствующих графиков (рис.1).

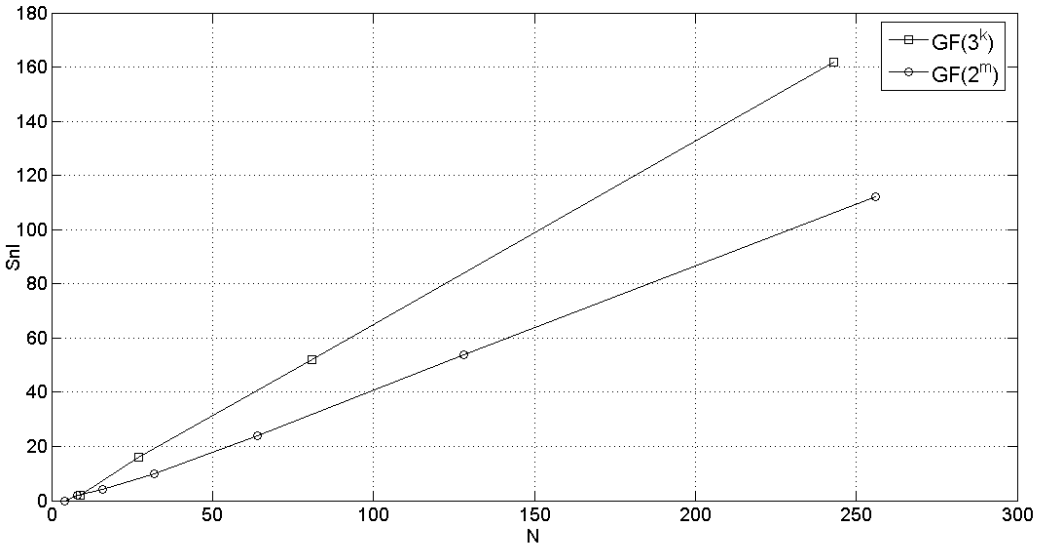

Рис.1

Анализ данных рис.1 позволяет сделать вывод: расстояние нелинейности S-блоков подстановки конструкции Ниберг над полями $GF(3^k)$ растет быстрее, нежели над полями $GF(2^m)$, что говорит о существенно большей стойкости к линейному криптоанализу в сравнении с той же конструкцией над полем характеристики 2.

Основные результаты проведенных исследований.

1. Дальнейшее развитие получил метод синтеза S-блоков подстановки конструкции Ниберг, в рамках чего построены S-блоки подстановки над полями $GF(3^k)$ для значений $k = 2,3,4,5$.

2. Введено понятие расстояния нелинейности S-блока подстановки длины $N = 3^k$ в терминах функций p-логики, которое обобщает понятие расстояния нелинейности булевой функции. Вычислены значения расстояния нелинейности для построенных S-блоков подстановки конструкции Ниберг над полями $GF(3^k)$.

3. Показано, что с ростом N расстояние нелинейности S-блоков подстановки конструкции Ниберг над полями Галуа характеристики $p = 3$ растет существенно быстрее, в сравнении с полями характеристики $p = 2$, а это является ценным с практической точки зрения.

Таким образом, построенные S-блоки подстановки могут быть рекомендованы для использования в существующих криптографических алгоритмах, а также для построения новых перспективных алгоритмов шифрования.

Заключительные замечания.

1**.** Как нетрудно заметить, проведенные рассуждения и вычисления с небольшими и достаточно очевидными изменениями распространяются на поля любой характеристики. При этом представляется интересным вопрос о соотношении количества раундов, необходимых для достижения близких значений параметров качества при разных значениях характеристик.

2. Как известно, оценка качества S-блока зависит от выбора критерия. В связи с этим отметим работу [10], где приведен пример для поля $GF(2^8)$: применение полинома

(десятичный эквивалент) 355 наиболее затруднит аппроксимацию шифра аффинными булевыми функциями, а применение полинома 425 наиболее затруднит корреляционный криптоанализ, однако упростит аппроксимацию аффинными булевыми функциями. Актуальной является задача полного описания соотношений между критериями как для поля характеристики $p = 2$, так и для полей характеристик $p = 3,5$.

3. До сих пор во всех известных публикациях рассматривались блоки замен, построенные на одном для всех раундов выбранном неприводимом полиноме. Однако, имеет смысл строить блоки замен, выбирая для каждого раунда новый полином. Исследование криптографического качества композиций преобразований, построенных на различных полиномах, может дать интересные результаты, хотя эта задача и представляется весьма трудоемкой.

Литература

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

2. Соколов, А.В. Новые методы синтеза нелинейных преобразований современных шифров / А.В. Соколов. – Lap Lambert Academic Publishing, Germany, 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.* Practical S-box design / S. Mister, C. Adams // Proceedings, Workshop in selected areas of cryptography, SAC’96, 1996. — P. 61—76.

5. *Медведева, Т.Е.* Оценка криптостойкости таблиц замен алгоритма ГОСТ 28147-89. / Т.Е. Медведева // Решетневские чтения, 2012. — С.666.

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

7. FIPS 197. [Electronic resource] Advanced encryption standard. — 2001. — http://csrc.nist.gov/publications/— 01.02.2015.

8. *Nyberg, K.* Differentially uniform mappings for cryptography. Advances in cryptology / K. Nyberg //Proc. of EUROCRYPT’93. — Berlin, Heidelberg, New York. — 1994. — vol.765, Lecture Notes in Compuer Springer-Verlag. — P.55 — 65.

9. *Мазурков, М.И.* Нелинейные преобразования на основе полных классов изоморфных и автоморфных представлений поля GF(256) / М.И. Мазурков, А.В. Соколов // Известия высших учебных заведений. Радиоэлектроника. — 2013. — Т. 56, N 11. — С. 16—24.

10. *Мазурков М.И.* Криптографические свойства нелинейного преобразования шифра Rijndael на базе полных классов неприводимых полиномов / М.И. Мазурков, А.В. Соколов. — Праці Одеського політехнічного університету, 2012. — Вип. 2(39). — С.183—189.

11. *Амбросимов, А.С.* Свойства бент-функций q-значной логики над конечными полями / А.С. Амбросимов // Дискрет. матем., 1994. — Т.6. — вып. 3. — С. 50—60.

12. *Лидл, Р.* Конечные поля / Р. Лидл, Г. Нидеррайтер. — М.: МИР, 1988. — 808 с.

13. Kim Y.S. On p-ary Bent Functions defined on Finite Fields / Y.S. Kim, J.W. Jang, J.S. No, T. Helleseth /, Proceedings of Mathematical Properties of Sequences and Other Combinatorial Structures (GolombFest 70), 2002. — P. 65—76.

14. Zhdanov O.N. Block symmetric cryptographic algorithm based on principles of variable block length and many-valued logic / O.N. Zhdanov, A.V. Sokolov. — Far East Journal of Electronics and Communications, 2016. — Vol. 16. — No. 3. — P. 573 — 589.