УДК 681.3.06

[1]*А. В. СОКОЛОВ*, [2]*О. Н. ЖДАНОВ*

НЕЛИНЕЙНЫЕ ПРЕОБРАЗОВАНИЯ КОНСТРУКЦИИ НИБЕРГ НАД ИЗОМОРФНЫМИ ПРЕДСТАВЛЕНИЯМИ ПОЛЕЙ ГАЛУА

[1] Одесский национальный политехнический университет
[2] Сибирский государственный аэрокосмический университет им. академика М. Ф. Решетнева

Дальнейшее развитие криптографических алгоритмов, основанных на принципах многозначной логики, требует более тщательного изучения недвоичных криптографических примитивов – S-блоков. Одной из перспективных конструкций для синтеза S-блоков является конструкция Ниберг, обеспечивающая высокое качество конструируемых S-блоков в двоичном случае. Недостатком конструкции Ниберг являются малые мощности конструируемых классов S-блоков. Тем не менее, данный недостаток удается преодалеть за счет рассмотрения всех изоморфных представлений основного поля, существенно расширив выбор доступных высококачественных S-блоков. Проведенные в настоящей статье исследования показали, что преимущества конструкции Ниберг могут быть легко перенесены на многозначный случай. Так, в работе построены полные множества S-блоков конструкции Ниберг над всеми изоморфными представлениями полей $GF(p^k)$, $p = 3,5$ и исследованы их нелинейные характеристики. В качестве критерия нелинейности выбран метод, основанный на измерении расстояния нелинейности: расстояния от компонентных функций многозначной логики до множества функций Виленкина-Крестенсона, являющихся наиболее линейными. Рассчитаны также коэффициенты корреляции векторов выхода и входа полученных S-блоков. Проведенные исследования показали высокое качество построенных криптографических примитивов и позволяют рекомендовать их к использованию в криптоалгоритмах, основанных на принципах многозначной логики.

Ключевые слова: *S-блок, конструкция Ниберг, многозначная логика.*

Введение

Стремительное развитие криптографических методов шифрования информации и их повсеместное распространение диктует необходимость дальнейшего развития общей теории криптографии, в частности, синтеза новых криптографических примитивов для увеличения эффективности современных шифров.

Одним из важнейших элементов блочного симметричного алгоритма шифрования является *S*-блок, его качество во многом определяет качество и быстродействие самого шифра. Более того, в некоторых алгоритмах шифрования, например, в ГОСТ 28147-89, который является достаточно актуальным и по сей день, *S*-блок является элементом ключевой информации.

Гибкий подход к выбору *S*-блоков имеет достаточно большое количество преимуществ, в частности, возможности дальнейшего улучшения и совершенствования криптоалгоритма, а также реализации концепции оперативной смены ключа.

Существование криптоалгоритмов с гибким подходом к выбору ключевой информации, а также активная разработка новых криптоалгоритмов требуют дальнейшего совершенствования существующих методов синтеза *S*-блоков и разработки новых.

Более того, развитие принципов многозначной логики, а также их адаптация к работе на двоичных вычислительных машинах, в последнее время привела к стремительному развитию недвоичной теории помехоустойчивого кодирования, недвоичной теории сигналов и недвоичных алгоритмов шифрования [1–3]. Конструирование недвоичных криптографических примитивов помимо высокой практической ценности также ведет к более глубокому пониманию принципов их работы и тем самым к дальнейшему развитию теоретической криптографии.

В настоящее время известны методы синтеза оптимальных недвоичных *S*-блоков, основанные на схеме Кима [4]. Тем не менее, данные *S*-блоки являются оптимальными только по критерию минимума коэффициентов корреляции векторов выхода и входа, тогда как их нелинейные характеристики весьма посредственны.

С другой стороны, известен метод синтеза двоичных *S*-блоков конструкции Ниберг над всеми изоморфными представлениями полей $GF(2^k)$, позволяющий получить большие множества подстановочных конструкций со сбалансированным уровнем криптографического качества [5].

Целью настоящей статьи является обобщение конструкции Ниберг на все изоморфные представления полей Галуа $GF(p^k)$, $p = 3,5$.

Конструкция Ниберг и её свойства

Оригинальная конструкция Ниберг представляет собой отображение, задаваемое мультипликативно обратными элементами поля Галуа $GF(2^k)$:

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

скомбинированное вместе с аффинным преобразованием

$$b = Ay + a,\ a, b \in GF(2^k), \quad (2)$$

где $f(z)$ – неприводимый над полем $GF(2)$ полином степени k; $0^{-1} \equiv 0$ – по определению; A – невырожденная матрица аффинного преобразования; a – вектор сдвига; $p = 2$ – характеристика расширенного поля Галуа; a, b, x, y – элементы расширенного поля Галуа $GF(2^k)$; мы можем их трактовать как десятичные числа, либо двоичные векторы, либо полиномы степени $k - 1$.

Структура *S*-блока во многом зависит от вида используемого неприводимого полинома $f(z)$, а количество неприводимых полиномов определяет мощность класса *S*-блоков конструкции Ниберг. Известно, что количество $|W_k|$ неприводимых над полем $GF(q)$ полиномов степени k, а также количество $|V_k|$ существующих среди них первообразных полиномов вычисляются по формулам

$$|W_k| = \frac{1}{k} \sum_{\substack{d \\ d/\mathrm{k}}} \mu(d)\, q^{(k/d)},\ |V_k| = \frac{\varphi(q^k - 1)}{k}, \quad (3)$$

где d – делители числа k, $\mu(d)$ – функция Мёбиуса, а запись d/k означает, что d делит k, φ – функция Эйлера.

Выбор аффинного преобразования является отдельной задачей, решаемой в зависимости от структуры *S*-блока и конкретных свойств, которые разработчики хотят получить с помощью аффинного преобразования, например, увеличение периода возврата *S*-блока в исходное состояние, уменьшение корреляционной связи выхода и входа, улучшение дифференциальных свойств *S*-блока [6]. Задача выбора аффинного преобразования выходит за пределы проведенного исследования и в данной статье авторами не рассматривается.

В целом, *S*-блоки конструкции Ниберг обладают высоким расстоянием нелинейности, хорошими корреляционными и дифференциальными свойствами.

Таким образом, *S*-блоки конструкции Ниберг идеально подходят для применения в криптоалгоритмах, основанных на принципах многозначной логики. Соответственно, актуальной является задача конструирования их множеств и подробного изучения их криптографических свойств.

Одним из немногих недостатков конструкции Ниберг является малое количество *S*-блоков, которое может быть получено таким методом. В полях $GF(2^k)$ данный недостаток удалось устранить путем рассмотрения всех изоморфных представлений поля, при этом криптографические свойства построенных *S*-блоков остаются стабильными. Исследования, проведенные в данной статье, показывают, что такой подход может быть распространен и на поля нечетной характеристики.

Изоморфные представления основного поля $GF(3^k)$

Как хорошо известно, поля $GF(3^k)$ тоже можно представить в виде различных изоморфных представлений. В настоящей работе рассмотрены поля $GF(3^k)$ и все их изоморфные представления для значений $k = 2$–7, что отражает практически ценные длины *S*-блоков. С учетом новых видов представления основного поля $GF(3^k)$ выражение (1) принимает вид

$$y = x^{-1} \bmod[f_1(z), f_2(z), p],\ y, x \in GF(3^k), \quad (4)$$

где $f_1(z)$ – неприводимый полином, определяющий операцию мультипликативного обращения в поле «нижнего уровня» $GF(q)$, $f_2(z)$ – в поле «верхнего уровня», т. е. расширении поля $GF(q^k)$.

Различные представления основного поля $GF(3^k)$, а также количества неприводимых и первообразных полиномов, существующих в данных полях, приведены в табл. 1.

Неприводимые и первообразные полиномы для полей $GF(3^k)$ можно найти в работе [7], тогда как нахождение полиномов для полей $GF(9^k)$ и $GF(27^k)$ представляет собой весьма интересную задачу, которая может быть решена с использованием метода [8]. Найденные неприводимые полиномы над $GF(9)$ приведены в табл. 2

Исследование криптографического качества построенных *S*-блоков

Одним из важнейших критериев криптографического качества подстановочных конструкций является их расстояние нелинейности, которое в двоичном случае измеряется как расстояние Хэмминга между компонентными функциями *S*-блока и всеми кодовыми словами аффинного кода.

Определение. *Аффинной* называется функция аналитического вида

Таблица 1. **Мощности множеств неприводимых и первообразных полиномов над полями $GF(3^k)$**

Основное поле	Возможные изоморфные представления	Количество неприводимых полиномов	Количество первообразных полиномов	Общее количество *S*-блоков
$GF(3^2)$	$GF(3^2)$	3	2	3
$GF(3^3)$	$GF(3^3)$	8	4	8
$GF(3^4)$	$GF(3^4) \Rightarrow GF(9^2)$	$18 \Rightarrow 36$	$8 \Rightarrow 16$	54
$GF(3^5)$	$GF(3^5)$	48	22	48
$GF(3^6)$	$GF(3^6)$, $GF(9^3)$, $GF(27^2)$	$116 \Rightarrow 240 \Rightarrow 351$	$48 \Rightarrow 96 \Rightarrow 144$	2000

Таблица 2. **Неприводимые и первообразные полиномы**

Поле	Полином $f_1(z)$	Полиномы $f_2(z)$
$GF(9^2)$	$f_1(z) = x^2 + x + 2$	84,86,87,88,**93**,94,**97**,98,**102**,103,**106**,107,109,110,**114**,**115**,121,**122**,**123**,125,127,128,**129**,**131**, 136,137,**141**,**142**,145,146,**147**,**149**,157, **158**,**159**,161
	$f_1(z) = x^2 + 2x + 2$	84,85,87,89,**94**,95,**96**,97,**103**,104,**105**,106,109,110,**111**,**112**,118, 119,**123**,**125**,**129**,131,133,**134**, 136,137,**138**,**139**,**147**,149,151,**152**,154,155,**159**,**161**
$GF(9^3)$	$f_1(z) = x^2 + x + 2$	741,742,743,744,745,746,748,749,750,752,753,754,766,767,768,769,771,773,802,803,805,806, 808,809,812,814,818,821,823,827,829,831,835,838,842,845,848,851,853,856,858,862,865,867, 871,874,877,879,884,885,888,892,895,899,901,904,908,911,914,915,920,922,925,928,932,934, 938,941,942,947,950,951,956,957,962,964,966,969,975,977,978,982,983,986,994,995,998, 1001,1006,1007,1011,1013,1014,1019,1024,1025,1027,1032,1033,1038,1039,1042,1046,1051, 1052,1054,1055,1057,1065,1067,1070,1072,1073,1075,1083,1085,1088,1093,1094,1096,1099, 1105,1106,1109,1113,1115,1119,1121,1124,1128,1129,1131,1137,1139,1141,1144,1145,1146, 1155,1156,1160,1165,1166,1167,1171,1176,1178,1181,1185,1186,1189,1194,1196,1198,1203, 1205,1209,1211,1213,1218,1221,1222,1225,1226,1231,1237,1240,1241,1243,1246,1247,1254, 1257,1258,1261,1264,1265,1271,1272,1274,1283,1284,1286,1288,1291,1292,1301,1302,1303, 1306,1307,1311,1318,1320,1322,1326,1330,1331,1334,1335,1336,1342,1344,1346,1352,1353, 1354,1361,1362,1363,1373,1374,1375,1378,1379,1385,1390,1392,1393,1396,1397,1403,1408, 1410,1411,1418,1420,1421,1424,1426,1427,1432,1434,1435,1444,1446,1447,1452,1455,1457
	$f_1(z) = x^2 + 2x + 2$	741,742,743,744,745,746,748,749,750,751,753,755,775,776,778,779,781,782,793,794,795,797, 798,799,812,815,817,821,824,826,829,832,834,838,841,843,847,849,853,857,858,861,865,869, 872,875,877,881,883,886,888,892,896,898,901,905,907,911,912,917,920,921,926,929,932,933, 937,939,942,947,949,952,955,958,962,965,966,971,975,976,978,982,983,985,994,995,997,1001, 1005,1007,1011,1013,1016,1018,1024,1025,1027,1033,1034,1038,1039,1041,1045,1051,1052, 1056,1057,1061,1063,1064,1065,1074,1076,1078,1082,1086,1087,1091,1095,1096,1101,1102, 1106,1111,1112,1113,1118,1122,1123,1126,1131,1133,1135,1136,1139,1146,1147,1150,1153, 1154,1157,1162,1167,1168,1173,1174,1177,1182,1184,1185,1191,1192,1195,1201,1202,1205, 1208,1213,1214,1218,1221,1223,1225,1226,1232,1238,1240,1241,1243,1245,1246,1255,1257, 1258,1262,1264,1265,1271,1273,1274,1281,1284,1286,1289,1291,1292,1297,1298,1303,1310, 1311,1313,1315,1316,1321,1325,1326,1328,1337,1338,1340,1344,1347,1348,1355,1356,1358, 1363,1366,1367,1369,1372,1373,1381,1383,1385,1387,1388,1392,1400,1401,1402,1405,1407, 1409,1414,1416,1418,1426,1428,1430,1434,1438,1439,1441,1443,1445,1451,1452,1453

$$\varphi(x_0,\ldots,x_{k-1}) = a_0x_0 + a_1x_1 + \ldots$$
$$+a_{k-1}x_{k-1} + b(\mathrm{mod}\ p) = \sum_{i=0}^{k-1} a_ix_i + b(\mathrm{mod}\ p), \quad (5)$$

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

Задача определения расстояния нелинейности для *S*-блоков подстановки многозначной логики является более сложной в виду их более сложной и многогранной природы.

Существенный прогресс в этом направлении был достигнут в работе [10], за счет использования коэффициентов нелинейности. Изложим кратко суть данного метода.

Пусть, например, задана произвольная 3-функция длины $N = 9$ в виде своей таблицы истинности

$$A = \left\{e^{2j\pi/3}\, e^{j0}\, e^{4j\pi/3}\, e^{2j\pi/3}\, e^{j0}\, e^{4j\pi/3}\, e^{2j\pi/3}\, e^{j0}\, e^{4j\pi/3}\right\}, \quad (6)$$

мы можем найти её спектральные коэффициенты Виленкина-Крестенсона

$$\Omega_A = A\overline{V}_9 = \left\{0\ 0\ 9e^{2j\pi/3}\ 0\ 0\ 0\ 0\ 0\ 0\right\}. \quad (7)$$

Поскольку полный троичный код может быть рассмотрен как линейное векторное пространство, в котором функции Виленкина-Крестенсона являются ортонормированным базисом, для преобразования Виленкина-Крестенсона справедливо равенство Парсеваля

$$\sum_{\omega=1}^{N} \left|\Omega(\omega)\right|^2 = 3^{2k}, \quad (8)$$

где k – количество переменных, от которых зависит эквивалентная 3-функция, $k = \log_3 N$ и $k = n = \sqrt{N}$ для троичных бент-функций.

Минимальное же значение коэффициентов преобразования Виленкина-Крестенсона достигается тогда, когда их значения постоянны по модулю и равны

$$\left|\Omega(\omega)\right| = \sqrt{\frac{3^{2k}}{3^k}} = 3^{k/2}, \quad \omega = 0,1,...,N-1. \quad (9)$$

Таким образом, нелинейность функций q-значной логики оценивается как разность между максимально возможным значением модуля коэффициента преобразования Велинкина-Крестенсона и максимальным значением (по модулю) преобразования Виленкина-Крестенсона исследуемой функции

$$NL = \begin{cases} q^k - \max\left\{\left|\Omega\right|\right\}, & q > 2; \\ 2^{k-1} - \dfrac{1}{2}\max\left\{\left|W\right|\right\}, & q = 2. \end{cases} \quad (10)$$

С другой стороны, в работе [4], посвященной синтезу троичных *S*-блоков оптимальных по критерию корреляции между векторами выхода и входа для оценки степени взаимосвязи векторов данных, предложено использовать обобщенную формулу для вычисления коэффициента корреляции

$$\Psi_{\nu,\mu} = \frac{\sum_{t=1}^{N} x_{\nu,t}y_{\mu,t} - \frac{\sum_{t=1}^{N} x_{\nu,t}\sum_{t=1}^{N} y_{\mu,t}}{N}}{\sqrt{\left[\sum_{t=1}^{N} x_{\nu,t}{}^2 - \frac{\left(\sum_{t=1}^{N} x_{\nu,t}\right)^2}{N}\right]\left[\sum_{t=1}^{N} y_{\mu,t}{}^2 - \frac{\left(\sum_{t=1}^{N} y_{\mu,t}\right)^2}{N}\right]}},$$
$$\nu,\mu = 1, 2, ..., k, \quad (11)$$

где μ, ν – номера компонентных булевых функций исследуемого *S*-блока и тривиальной подстановки 0, 1, …, N – 1; $k = \log_p N$ – количество компонентных булевых функций.

Для проведения сравнительного анализа *S*-блоков удобно использовать коэффициент корреляционной связи векторов выхода и входа, определяемый как максимум среди модулей элементов матрицы $\rho = \max\left|\Psi_{\nu,\mu}\right|$.

Приведем пример исследования нелинейных свойств *S*-блока подстановки длины $N = 81$. Построим *S*-блок над полем $GF(9^2)$ на основе (4) и полиномов $f_1(z) = x^2 + x + 2$, $f_2(z) = 107_{10} = x^2 + 2x + 8$, который представим в виде *Q*-последовательности

$$Q = \{0\ \ 1\ \ 2\ \ 5\ \ 8\ \ 3\ \ 7\ \ 6\ \ 4\ 37\ 49\ 21\ 67\ 59$$
$$65\ 19\ 50\ 36\ 74\ 15\ 71\ 11\ 72\ 70\ 53\ 46\ 34$$
$$32\ 43\ 80\ 75\ 39\ 27\ 64\ 26\ 68\ 17\ \ 9\ 69\ 31\ 55$$
$$44\ 60\ 28\ 41\ 66\ 25\ 57\ 73\ 10\ 16\ 63\ 58\ 24$$
$$61\ 40\ 77\ 47\ 52\ 13\ 42\ 54\ 78\ 51\ 33\ 14\ 45\ 12$$
$$35\ 38\ 23\ 20\ 22\ 48\ 18\ 30\ 79\ 56\ 62\ 76\ 29\}. \quad (12)$$

Представим *S*-блок подстановки (12) в виде компонентных 3-функций

$$f_1 = \{000000000110222011202022111112211202002121211202200220212111012211010110001012222 1\};$$

$$f_2 = \{00000000012210122121112122001221012$$
$$111100100112021110201222110220121012222 2$$
$$020020\};$$
$$f_3 = \{00012122101111001002200220212211002$$
$$120210220112100201221102120222101201011 0$$
$$120210\};$$
$$f_4 = \{01222010111012212020220121121200012$$
$$220011201201011101011221100000200222210 0$$
$$012212\}. \quad (13)$$

Для каждой из 3-функций найдем коэффициенты преобразования Виленкина-Крестенсона. Например, модули спектральных коэффициентов преобразования Виленкина-Крестенсона первой компонентной 3-функции имеют вид

$$S_1 = \{0\ 9\ 0\ 3\ 6\ 12\ 6\ 12\ 6\ 15\ 3\ 6\ 9\ 9\ 9$$
$$15\ 12\ 3\ 6\ 6\ 3\ 3\ 3\ 12\ 9\ 9\ 0\ 3\ 3\ 6\ 12\ 6$$
$$3\ 9\ 9\ 9\ 18\ 9\ 9\ 12\ 3\ 3\ 3\ 3\ 15\ 15\ 15\ 3 \quad (14)$$
$$9\ 0\ 9\ 3\ 3\ 3\ 15\ 6\ 15\ 9\ 9\ 9\ 12\ 15\ 6\ 3\ 3$$
$$3\ 6\ 15\ 6\ 9\ 9\ 9\ 18\ 0\ 9\ 15\ 3\ 15\ 12\ 6\ 3\}.$$

Для *S*-блока (12) максимум модуля по всем спектральным коэффициентам равен $L = \max\{S\} = 18$, таким образом, можем вычислить коэффициент нелинейности по формуле $NL = q^k - \max\{|S|\} = 3^4 - 18 = 63$, что является неплохим результатом. Для сравнения, для данной длины коэффициент нелинейности бент-функций равен $NL_{\max} = 3^4 - \sqrt{3^4} = 72$.

В табл. 3 представлены результаты расчета коэффициентов нелинейности *NL*, а также максимумов коэффициентов корреляции векторов выхода и входа ρ троичных *S*-блоков конструкции Ниберг над различными изоморфными представлениями полей $GF(3^k)$.

Важно заметить, что коэффициенты корреляции могут различаться и *для разных представлений одного поля.*

Случай характеристики 5

Основные поля для практически ценных значений *k* также имеют различные свои изоморфные представления (табл. 4), где рядом указаны количества неприводимых и первообразных неприводимых полиномов.

Для того, чтобы оценить криптографические характеристики *S*-блоков подстановки конструкции Ниберг, основанных на принципах 5-логики, необходимо построить таблицы (табл. 5) первообразных (выделены жирным шрифтом) и неприводимых полиномов для расширенных полей $GF(5^k)$, для чего воспользуемся алгоритмом [8].

Основываясь на приведенных полиномах и методе построения *S*-блоков подстановки конструкции Ниберг, можем оценить их крип-

Таблица 3. **Качество *S*-блоков конструкции Ниберг над полями $GF(3^k)$**

Поле	Изоморфное представление		*NL*	ρ
$GF(3^2)$	$GF(3^2)$		3	0.8333
$GF(9^3)$	$GF(3^3)$		18	0.2222–0.3333
$GF(3^4)$	$GF(3^4)$		63	0.1667–0.3333
	$GF(9^2)$		63	0.2037–0.3333
$GF(3^5)$	$GF(3^5)$		213	0.0617–0.1543
$GF(3^6)$	$GF(3^6)$		675	0.0453–0.0986
	$GF(9^3)$	Полином $GF(9)x^2 + x + 2$	675	0.0432–0.0967
		Полином $GF(9)x^2 + 2x + 2$	675	0.0514–0.0967
	$GF(27^2)$	Полином $GF(27)x^3 + 2x + 1$	675	0.0885–0.0967
		Полином $GF(27)x^3 + x^2 + 2x + 1$	675	0.0761–0.0967
		Полином $GF(27)x^3 + 2x^2 + 1$	675	0.0885–0.0967
		Полином $GF(27)x^3 + 2x^2 + x + 1$	675	0.0761–0.0967

Таблица 4. **Мощности множеств неприводимых и первообразных полиномов над полями $GF(5^k)$**

Основное поле	Возможные изоморфные представления	Количество неприводимых полиномов	Количество первообразных полиномов	Общее количество *S*-блоков конструкции Ниберг
$GF(5^2)$	$GF(5^2)$	10	4	10
$GF(5^3)$	$GF(5^3)$	40	20	40
$GF(5^4)$	$GF(5^4) \Rightarrow GF(25^2)$	$150 \Rightarrow 300$	$48 \Rightarrow 96$	1350

Таблица 5. **Неприводимые и первообразные полиномы над полем *GF*(5)**

Поле	Полиномы
$GF(5^2)$	27,28,31,**32**,**38**,39,**43**,44,46,**47**
$GF(5^3)$	131,134,136,139,**142**,**143**,**147**,**148**,151,**152**,**158**,159,166,169,171,**173**,176,**178**,**183**,184,**187**,**188**,**197**,199,**202**,204, 206,**207**,**212**,**213**,221,**223**,**228**,229,231,**232**,241,244,**247**,249
$GF(5^4)$	627,628,634,639,644,649,652,656,**662**,**663**,**667**,**668**,671,678,686,688,691,693,703,706,708,721,723,727,**732**,**733**, 736,741,**747**,**748**,754,**758**,**763**,764,**767**,771,**772**,776,**783**,784,789,793,797,**802**,**807**,808,811,812,819,824,826,**828**, 836,**847**,849,852,856,859,871,**873**,879,**883**,884,886,**887**,**893**,**897**,902,911,**913**,916,919,926,**928**,931,**937**,939,**952**, 956,957,964,**967**,968,974,976,984,987,**993**,994,998,1004,**1007**,**1013**,1016,**1017**,**1023**,1024,1027,1036,1039,1041, **1043**,1051,**1053**,**1067**,1069,1071,**1077**,1084,**1087**,1088,1094,1096,1097,1101,1108,**1113**,1114,1117,1124,1129, 1131,**1132**,**1137**,**1143**,1144,**1148**,1151,1157,1163,1169,**1173**,1174,**1177**,1184,1189,1191,1192,**1197**,1198,1201, **1203**,**1207**,1209,1216,1227,1231,**1233**,1246,1249

Таблица 6. **Качество *S*-блоков конструкции Ниберг над полями $GF(5^k)$**

Изоморфное представление			NL	ρ
$GF(5^2)$			14.1459	0.28–0.72
$GF(5^3)$			103.8197	0.048–0.24
$GF(5^4)$	$GF(5^4)$		574.2229	0.0368–0.3869
	$GF(25^2)$	Полином $GF(25)x^2 + x + 2$	574.2229	0.0768–0.1384
		Полином $GF(25)x^2 + 2x + 3$	574.2229	0.0768–0.1384
		Полином $GF(25)x^2 + 3x + 3$	574.2229	0.0768–0.1384
		Полином $GF(25)x^2 + 4x + 2$	574.2229	0.0768–0.1384

тографическое качество в соответствии с изложенной выше методикой.

Таким образом, качество *S*-блоков подстановки конструкции Ниберг над всеми изоморфными представлениями полей $GF(5^k)$ также является высоким и стабильным с точки зрения нелинейности.

Заключение

1. В статье построены полные множества *S*-блоков подстановки над всеми изоморфными представлениями полей $GF(p^k)$, $p = 3{,}5$. Относительно построенных множеств *S*-блоков проведены исследования нелинейности на основе коэффициентов преобразования Виленкина-Крестенсона и коэффициентов корреляции выхода и входа. Проведенные исследования показали высокое качество полученных *S*-блоков и относительную стабильность их характеристик.

2. Построены и табулированы полные множества неприводимых и первообразных полиномов над полем *GF*(5) до четвертой степени включительно, которые могут быть использованы не только для построения *S*-блоков, но также и для построения генераторов псевдослучайных ключевых последовательностей.

3. Построенные *S*-блоки в силу своего высокого качества могут быть рекомендованы к использованию в новейших криптографических алгоритмах, основанных на принципах многозначной логики.

4. Построение аналогичных конструкций полей характеристики больше 5 не представляет затруднений, однако, является, на наш взгляд, менее актуальным в аспекте применений.

Литература

1. 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.

2. Кузнецов, В. С. Троичные каскадные коды с модуляцией кам-9 и их возможности / В. С. Кузнецов. – «Инфо-Электросвязь», 2009. – С. 30–33.

3. Петелин, Ю. В. Перспективы использования сигнально-кодовых конструкций типа троичных М-последовательностей в спутниковых каналах связи / Ю. В. Петелин, М. А. Ковалев, А. А. Макаров // Информационно-управляющие системы. – 2006. – №. 5. – С. 32–35.

4. Жданов, О. Н. Алгоритм построения оптимальных по критерию нулевой корреляции недвоичных блоков замен / О. Н. Жданов, А. В. Соколов. – Проблемы физики, математики и техники, 2015. – № 3(24). – С. 94–97.

5. 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.

6. Мазурков, М. И. Нелинейные S-блоки конструкции Ниберг с максимальным лавинным эффектом / М. И. Мазурков, А. В. Соколов // Известия высших учебных заведений. Радиоэлектроника. – 2014. – Т. 57, N 6. – С. 47–55.

7. Соколов, А. В. Генератор псевдослучайных ключевых последовательностей на основе тройственных наборов бент-функций / А. В. Соколов, О. Н. Жданов, Н. А. Барабанов. – Проблемы физики, математики и техники, 2016. – № 1 (26). – С. 85–91.

8. Мазурков М. И. Конструктивный способ построения первообразных неприводимых полиномов над простыми полями Галуа / М. И. Мазурков // Радиоэлектроника. – 1999. – № 2. – С. 41–45. (Изв. вузов).

9. Юровских, Д. А. Полуторабайтные нелинейные преобразования конструкции Ниберг / Д. А. Юровских, А. В. Соколов, Б. С. Троицкий. – Информатика и математические методы в моделировании. – 2016. – Т. 6. – № 2. – С. 142–148.

10. Sokolov, A. V. Regular synthesis method of a complete class of ternary bent-sequences and their nonlinear properties / A. V. Sokolov, ON Zhdanov. – Journal of Telecommunication, Electronic and Computer Engineering. – VOL 8. – No 9. – P. 39–43.

References

1. 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.

2. Kuznetsov, V. S. Ternary cascade codes with QAM-9 modulation and their possibilities / V. S. Kuznetsov. – «Info-Electrosvyaz», 2009. – P. 30–33.

3. Petelin, Yu. V. Prospects of the use of signal-code constructions of the type of ternary M-sequences in satellite communication channels / Yu. V. Petelin, M. A. Kovalev, A. A. Makarov // Information-control systems. – 2006. – No 5. – P. 32–35.

4. Zhdanov, O. N. Algorithm of construction of optimal according to criterion of zero correlation nonbinary *S*-boxes / O. N. Zhdanov, A. V. Sokolov. – Problems of physics, mathematics and technics, 2015. – No 3 (24). – P. 94–97.

5. Mazurkov, M. I. Nonlinear transformations based on complete classes of isomorphic and automorphic representations of field GF(256) / M. I. Mazurkov, A. V. Sokolov // Radioelectronics and Communications Systems. – 2013. – Vol. 56, No 11. – P. 513–521.

6. Mazurkov, M. I. Non-linear S-box of Nyberg construction with maximal avalanche effect / M. I. Mazurkov, A. V. Sokolov // Radioelectronics and Communications Systems. – 2014. – Vol. 57, No 6. – P. 274–281.

7. Sokolov, A. V. Pseudo-random key sequence generator based on triple sets of bent-functions / A. V. Sokolov, O. N. Zhdanov, N. A. Barabanov. – Problems of physics, mathematics and technics, 2016. – No. 1 (26). – P. 85–91.

8. Mazurkov M. I. A constructive method for constructing of primitive irreducible polynomials over simple Galois fields / Mazurkov // Radioelectronics. – 1999. – No 2. – P. 41–45.

9. Yurovskikh, D. A. Niberg construction 12 bit nonlinear transforms / DA. Yurovsky, A. V. Sokolov, B. S. Troitsky. – Informatics and mathematical methods in modeling. – 2016. – T. 6. – No 2. – P. 142–148.

10. Sokolov, A. V. Regular synthesis method of a complete class of ternary bent-sequences and their nonlinear properties / A. V. Sokolov, ON Zhdanov. – Journal of Telecommunication, Electronic and Computer Engineering. – VOL 8. – No 9. – P. 39–43.

Поступила	*После доработки*	*Принята к печати*
30.05.2017	*06.06.2017*	*10.09.2017*

Zhdanov O. N., Sokolov A. V.

NONLINEAR NYBERG CONSTRUCTION TRANSFORMS OVER ISOMORPHIC REPRESENTATIONS OF FIELDS GALOIS

Further development of cryptographic algorithms based on the principles of many-valued logic requires more accurate research of non-binary cryptographic primitives – S-boxes. One of the most promising constructions for the synthesis of S-boxes is the Nyberg construction, which ensures high quality of the designed S-boxes in the binary case. The disadvantage of the Nyberg construction is the small cardinality of the classes of the constructed S-boxes. Nevertheless, this disadvantage can be overcome by considering all the isomorphic representations of the main field, substantially expanding the choice of available high-quality S-boxes. The research carried out in this paper has shown that the advantages of the Nyberg construction can be easily transferred to a many-valued case. Thus, we construct complete sets of S-boxes of the Nyberg construction over all isomorphic representations of fields GF(p^k), p = 3,5, and research their nonlinear characteristics. As a criterion of nonlinearity, we measure the distances from the component many-valued functions to the set of Vilenkin–Chrestenson functions that are considered to be the most linear. The correlation coefficients of the output and input vectors of the obtained S-boxes are calculated. The researches performed have shown the high quality of the constructed cryptographic primitives and allow recommendation of them for use in cryptoalgorithms based on the principles of many-valued logic.

Keywords: *S-box, Nyberg construction, many-valued logic.*

Артем Соколов родился 15 апреля 1990 года в Одессе, УССР. Получил степень бакалавра (с отличием) по специальности «Системы технической защиты информации» в 2011 году, степень магистра (с отличием) по специальности «Системы технической защиты информации, автоматизация её обработки» в 2013 году и степень кандидата технических наук по специальности «Системы защиты информации» в 2014 году в Одесском национальном политехническом университете, г. Одесса, Украина.

С 2012 по 2014 работал младшим научным сотрудником кафедры Информационной безопасности в Одесском национальном политехническом университете. С 2014 года является старшим преподавателем кафедры Информационной безопасности, с 2016 – кафедры Радиоэлектронных и телекоммуникационных систем Одесского национального политехнического университета. Является автором монографии и более 70 научных публикаций. Научные интересы включают в себя методы защиты информации на основе совершенных алгебраических конструкций, методы синтеза алгоритмов шифрования данных и нелинейных S-блоков.

Артем Соколов награжден Золотой медалью за высокие достижения в учебе, Дипломом победителя в конкурсе Магистров, 2013 год; Дипломом победителя Всеукраинского конкурса научно-исследовательских работ «Телекоммуникационные системы и сети», 2012 год; Дипломом за высокие академические и исследовательские достижения, 2010 год.

Artem V. Sokolov was born in Odessa, USSR, in 1990. He received a Bachelor (Hons) degree in systems of technical data protection in 2011, Master (Hons) degree in systems of technical data protection and automation of it's processing in 2013 and Ph. D. degree in data protection systems in 2014 from Odessa National Polytechnic University, Odessa, Ukraine.

From 2012 to 2014 he was a Junior Researcher of the Data Security department in Odessa National Polytechnic University. Since 2014 he has been a Senior Lecturer of the Data Security Department in Odessa National Polytechnic University and since 2016 is a Senior Lecturer of the Radioelectronic and telecommunication systems. He is the author of a book and more than 70 articles. His research interests include data protection methods based on perfect algebraic constructions, nonlinear S-box synthesis method, and stream encryption algorithms.

A. V. Sokolov awards and honors include: Gold medal for high achievements in education, Hons Diploma of Winner in Master Competition, 2013; winner of «Information and communication networks» Ukrainian competition of research papers, 2012; Diploma for excellent academic and research activities, 2010.

Жданов Олег Николаевич родился 16 апреля 1964 года. В 1986 году окончил Красноярский Государственный Университет. Кандидатская диссертация по специальности «математический анализ» защищена в 1994 году. В настоящее время доцент кафедры безопасности информационных технологий Сибирского Государственного Аэрокосмического университета.

Читаемые лекционные курсы: «Криптографические методы защиты информации» (имеется удостоверение Института Криптографии, Связи и Информатики о соответствующем повышении квалификации), «Теоретико-числовые алгоритмы криптографии», «Теория надежности».

Общее количество публикаций 75, из них 7 – учебные пособия (в соавторстве с учениками).

Сфера научных интересов: системы дифференциальных уравнений в частных производных, являющиеся моделями процессов в механике сплошных сред. Получены точные решения уравнений пластичности плоского напряженного состояния, предложен новый подход к исследованию смешанной задачи для системы уравнений плоского напряженного состояния среды Мизеса, построен алгоритм нахождения решения задачи Коши для системы уравнений, описывающей одномерный поток гранулированного материала.

Еще одной областью научных интересов является защита информации: разработка реализации алгоритмов шифрования данных при передаче по открытому каналу с привлечением к этой работе студентов старших курсов для выполнения ими курсового и дипломного проектирования. Совместно с учениками разработал методику выбора ключевой информации для реализации алгоритмов блочного шифрования. Получено авторское свидетельство (совместно с Чалкиным Т. А.) на программный комплекс, реализующий выбор ключевой информации для шифрования данных по действующему стандарту России.

Два ученика стали лауреатами стипендии губернатора Красноярского края, а один – лауреат стипендии Правительства России и победитель конкурса на лучшую студенческую научную работу.

Награжден Благодарственным Письмом Законодательного Собрания Красноярского края. Награжден нагрудным знаком Министерства Образования и Науки РФ «За развитие научно-исследовательской работы студентов».

Zhdanov Oleg Nikolaevich was born on April 16, 1964. He graduated from Krasnoyarsk State University in 1986. The Ph. D. thesis in mathematical analysis was defended in 1994. At the moment O. N. Zhdanov is Associate Professor of Informational Technologies subdepartment of Siberian State Space University and associate professor of Algebra and mathematical logic department of Siberian Federal university.

O. N. Zhdanov gives the following lecture courses: «Cryptographic methods of information security» (there is a certificate of Institute of Cryptography, Communication and Information Sciences of the corresponding advanced training), «Number-theoretic algorithms of cryptography», «Reliability theory».

The total number of his publications – 75. Eight of them are study guides.

Together with pupils, he developed a key information choice method for realization of block encryption algorithms. Together with Chalkin T. A. he received the copyright certificate on the program complex realizing the choice of key information for data encryption according to the current standard of Russia.

O. N. Zhdanov was awarded by a letter of thanks from Legislative Assembly of Krasnoyarsk Krai, a breastplate of the Ministry of Education and Science of the Russian Federation «For development of students research activity».