УДК 681.3.06

МАЗУРКОВ М.И., СОКОЛОВ А.В.

НЕЛИНЕЙНЫЕ S -БЛОКИ КОНСТРУКЦИИ НИБЕРГ С МАКСИМАЛЬНЫМ ЛАВИННЫМ ЭФФЕКТОМ

Одесский национальный политехнический университет,
Украина, Одесса, 65044, пр. Шевченко 1

Аннотация. Построен полный класс неприводимых полиномов $f(z)$ восьмой степени над всеми изоморфными представлениями поля $GF(256)$. Найдено множество оптимальных пар $\{f(z), A\}$, где A — невырожденная матрица аффинного преобразования, что позволило существенно увеличить число S -блоков конструкции Ниберг, оптимальных по критерию максимального лавинного эффекта.

Abstract. The full class of irreducible polynomials $f(z)$ of eight degree over all isomorphic representations of Galois field $GF(256)$ is constructed. The set of optimal pairs $\{f(z), A\}$, where A — nonsingular affine transformation matrix is founded which allowed to significantly increase the number of Nyberg construction S-boxes, giving maximum avalanche effect.

Ключевые слова: S -блок, конструкция Ниберг, аффинное преобразование, критерий максимального лавинного эффекта; S -box, Nyberg construction, an affine transformation, the criterion of maximum avalanche effect.

Ключевым этапом разработки любого современного симметричного алгоритма шифрования является построение криптографически качественного нелинейного преобразования — S -блока, свойства которого определят устойчивость шифра к атакам линейного, корреляционного и дифференциального криптоанализа. В последнее время усиленное внимание уделяется вопросам синтеза нелинейных S -блоков конструкции, предложенной К. Ниберг [1], удовлетворяющих критерию максимального лавинного эффекта [2], применительно к шифру Rijndael/AES [3]. Нелинейные S -блоки конструкции Ниберг отвечающие максимальному лавинному критерию синтезируются путем выбора подходящей пары: вида неприводимого полинома $f(z)$ степени $\deg f(z) = 8$ и вида матрицы аффинного преобразования $y = Ax + b$. При этом в работе [2] применялись неприводимые над полем $GF(2^8)$ полиномы восьмой степени, число которых $\left| f_2^8 \right| = 30$.

Целью настоящей статьи является построение нелинейных S -блоков конструкции Ниберг, удовлетворяющих критерию максимального лавинного эффекта на основе полного класса неприводимых полиномов над всеми изоморфными представлениями поля $GF(256)$, применительно к шифру Rijndael/AES.

Для полноты изложения материала статьи приведем сущность метода построения S -блоков, удовлетворяющих критерию максимального лавинного эффекта [2]. Пусть $X = [x_i]$, $i = \overline{0,255}$, — последовательность возрастающих чисел от 0 до 255. Конструкция Ниберг отображает каждый элемент x_i в мультипликативно обратный элемент y_i по правилу

$$y_i \equiv x_i^{-1} \operatorname{modd}(f(z), 2),\ i = \overline{0,255}, \tag{1}$$

где в качестве $f(z)$ выберем неприводимый полином $f(z) = z^8 + z^6 + z^3 + z^2 + 1$;

$\operatorname{modd}(f(z), 2)$ — взятие по двойному модулю.

В результате получаем последовательность $Y = [y_i]$, $i = \overline{0,255}$, с другим порядком следования чисел y_i, отличным от порядка следования x_i, где принято, что $0^{-1} = 0$. Затем к элементам y_i последовательности Y применяется аффинное преобразование

$$q_i = Ay_i + b,\ i = \overline{0,255}, \tag{2}$$

где матрица A аффинного преобразования и вектор сдвига b в шифре Rijndael [1] имеют вид

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}, \quad \mathrm{b} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}. \tag{3}$$

Последовательность $Q = [q_i],\ i = \overline{0,255}$ представим с помощью таблицы истинности в виде её компонентных булевых функций

$$Q = [F_1; F_2; F_3; F_4; F_5; F_6; F_7; F_8], \tag{4}$$

где знак ";" означает вертикальную конкатенацию компонентных булевых функций длины $N = 256$ каждая. Найдем производные $D_{i,k} = F_i(x) \oplus F_i(x \oplus e_k)$ каждой булевой функции по каждому направлению e_k веса $wt(e_k) = 1$, где e_k — вектор с единицей на k-й позиции и нулями на остальных; $\oplus$ — операция суммирования по модулю 2. Построим таблицу (табл. 1) весов производных компонентных булевых функций $wt\left(D_{i,k}\right)$

Таблица 1

e_k	$wt\left(D_{1,k}\right)$	$wt\left(D_{2,k}\right)$	$wt\left(D_{3,k}\right)$	$wt\left(D_{4,k}\right)$	$wt\left(D_{5,k}\right)$	$wt\left(D_{6,k}\right)$	$wt\left(D_{7,k}\right)$	$wt\left(D_{8,k}\right)$
10000000	136	124	128	116	120	140	124	124
01000000	124	124	120	120	140	124	124	136
00100000	124	136	132	140	124	132	136	124
00010000	136	144	120	124	132	128	124	124
00001000	144	124	128	132	128	120	124	136
00000100	124	140	132	128	120	132	136	144
00000010	140	124	136	120	132	120	144	124
00000001	124	132	124	132	120	128	124	140

Определение [2]. Нелинейный S-блок обладает критерием максимального лавинного эффекта если все веса $wt\left(D_{i,k}\right)$ всех производных его компонентных булевых функций по всем направлениям единичного веса имеют значение, равное не меньше половины длины S-блока

$$wt\left(D_{i,k}\right) \geq N/2 = 128,\ i,k = \overline{1,8}. \tag{5}$$

Из анализа данных конструкции (табл.1) приходим к выводу о том, что S-блок (4) не обладает свойством максимального лавинного эффекта. Поэтому в работе [2] предложен следующий метод **M1** построения S-блоков, удовлетворяющих критерию максимального лавинного эффекта.

Шаг 1. Выберем произвольно невырожденную матрицу аффинного преобразования A, например из (3). Зафиксируем первые 7 её строк, а восьмибитное двоичное число, представляемое восьмой строкой, принимает значения от 0 до 255 т.е. все $2^8 = 256$ возможных значений. Найдем все такие структуры восьмой строки, при которых вес производной

$wt\left(D_{8,k}\right) \geq 128$. Найденные 10 структур восьмой строки поместим в множество Ψ, в шестнадцатеричной системе счисления

$$\Psi = \{0\text{D}, 1\text{B}, 24, 37, 52, 6\text{F}, 86, 92, \text{A}9, \text{DF}\}_h \ . \tag{6}$$

Установлено, что построение такой матрицы аффинного преобразования A, которая бы позволяла S-блоку конструкции Ниберг соответствовать критерию максимального лавинного эффекта возможно тогда, и только тогда, когда объем $|\Psi| \geq k$, что является необходимым условием.

Шаг 2. На основании данных множества (6) построим $C_{10}^{8} = 45$ квадратных матриц размера (8×8), из которых отберем 20 уникальных конструкций аффинного преобразования, позволяющих получить 20 уникальных S-блоков, удовлетворяющих критерию максимального лавинного эффекта. Например, рассмотрим одну из матриц $A = [1\text{B}, 37, 52, 6\text{F}, 86, 92, \text{A}9, \text{DF}]^T$, которая в двоичном виде представляется как

$$A = \begin{bmatrix} 1&1&0&1&1&0&0&0 \\ 1&1&1&0&1&1&0&0 \\ 0&1&0&0&1&0&1&0 \\ 1&1&1&1&0&1&1&0 \\ 0&1&1&0&0&0&0&1 \\ 0&1&0&0&1&0&0&1 \\ 1&0&0&1&0&1&0&1 \\ 1&1&1&1&1&0&1&1 \end{bmatrix}. \tag{7}$$

Применив данное преобразование (7) к S-блоку (4) получаем новый S-блок, удовлетворяющий критерию максимального лавинного эффекта, как это видно из анализа таблицы 2

Таблица 2

e_k	$wt\left(D_{1,k}\right)$	$wt\left(D_{2,k}\right)$	$wt\left(D_{3,k}\right)$	$wt\left(D_{4,k}\right)$	$wt\left(D_{5,k}\right)$	$wt\left(D_{6,k}\right)$	$wt\left(D_{7,k}\right)$	$wt\left(D_{8,k}\right)$
10000000	144	132	140	128	140	128	132	132
01000000	132	128	144	132	136	132	140	136
00100000	128	132	128	136	144	128	144	132
00010000	132	136	136	132	132	136	128	136
00001000	136	132	136	136	128	132	136	132
00000100	132	136	128	132	132	144	136	128
00000010	136	132	136	128	136	136	128	128
00000001	132	128	136	128	132	128	136	136

Шаг 3. Варьируя значения вектора сдвига b добиваемся наилучших корреляционных свойств S-блока. Экспериментально установлено, что структура вектора сдвига b не оказывает влияния на вид матрицы расстояний производных компонентных булевых функций. Очевидны модификации рассмотренного метода поиска подходящих аффинных преобразований для каждого неприводимого полинома $f(z)$.

Анализ данного метода также органично ставит задачу поиска таких неприводимых полиномов, для которых существует подходящая матрица аффинного преобразования A, при котором S-блок должен удовлетворять критерию максимального лавинного эффекта. Известно [4], что количество неприводимых полиномов степени k над полем $GF(q)$ определяется как

$$\left| f_q^k \right| = \frac{1}{k} \sum_{d \ \ k} \mu(d) \cdot q^{(k/d)} \ , \tag{8}$$

где d — делители числа k, $\mu(d)$ — функция Мёбиуса, а запись $d \ \ k$ означает, что d делит k. В криптоалгоритме Rijndael/AES, при значениях $q=2$, $k=8$ количество неприводимых полиномов, в соответствии с формулой (8) достигает $\left| f_2^8 \right| = 30$, что является криптографически незначительной величиной. Однако, в работе [5] предложен метод построения полного класса неприводимых полиномов над всеми изоморфными представлениями поля $GF(q)$. Например, рассмотрим поле $GF(256)$, которое имеет следующие свои изоморфные представления

$$GF(256) => GF(2^8) => GF(4^4) => GF(16^2), \tag{9}$$

среди которых в соответствии с выражением (8) в поле $GF(2^8)$ имеется $\left| f_2^8 \right| = 30$ неприводимых полиномов, в поле $GF(4^4)$ имеется $\left| f_4^4 \right| = 60$ неприводимых полиномов, а в поле $GF(16^2)$ имеется $\left| f_{16}^2 \right| = 720$ неприводимых полиномов. Таким образом, количество неприводимых полиномов над всеми изоморфными представлениями поля $GF(256)$ определяется как

$$J = \left| f_2^8 \right| + 1 \cdot \left| f_4^4 \right| + \left| f_{16}^2 \right| = 30 + 60 + 720 = 810 . \tag{10}$$

Проведенный экспериментальный анализ всех 810-ти криптографических S-блоков, построенных на базе всех неприводимых полиномов (10) показал, что для них характерны криптографически привлекательные свойства, а именно: равномерная минимизация матрицы коэффициентов корреляции, высокое расстояние нелинейности $N_s = 112$, высокая алгебраическая степень нелинейности $\deg(F_i) = 7$, $i = \overline{1,8}$.

Сведем в табл. 3 данные о количестве подходящих пар $\{f(z), A\}$, которые обеспечивают построение оптимальных S-блоков по критерию максимального лавинного эффекта.

Таблица 3

Изоморфное представление поля $GF(256)$	Неприводимый полином	$\lvert\Psi\rvert$	Количество подходящих матриц
$GF\left(2^8\right)$	$f(z)=z^8+z^6+z^3+z^2+1$	10	20
	$f(z)=z^8+z^6+z^5+z^2+1$	10	20
	$f(z)=z^8+z^6+z^5+z^4+z^3+z+1$	9	5
	$f(z)=z^8+z^7+z^5+z^4+z^3+z^2+1$	9	5
$GF\left(4^4\right)$	$f(z)=z^4+z^2+2z+3$	14	1073
	$f(z)=z^4+z^2+3z+2$	14	1073
	$f(z)=z^4+2z^2+2z+2$	14	723
	$f(z)=z^4+2z^2+3z+1$	16	5519
	$f(z)=z^4+3z^2+2z+1$	16	5519
	$f(z)=z^4+3z^2+3z+3$	14	723
	$f(z)=z^4+z^3+z^2+2$	14	723
	$f(z)=z^4+z^3+z^2+3$	14	723
	$f(z)=z^4+z^3+2z^2+z+1$	11	89
	$f(z)=z^4+z^3+3z^2+z+1$	11	89
	$f(z)=z^4+2z^3+3z^2+1$	16	5519
	$f(z)=z^4+2z^3+3z^2+3$	14	1073
	$f(z)=z^4+3z^3+2z^2+1$	16	5519
	$f(z)=z^4+3z^3+2z^2+2$	14	1073

Анализируя результаты табл. 3 нетрудно установить, что общее количество существующих над изоморфными представлениями поля $GF(256)$ S-блоков конструкции Ниберг, которые удовлетворяют критерию максимального лавинного эффекта, определяется величиной $V_1=29\,488$, из которых $V_2=50$ были построены в [2]. Найдено также, что неприводимые полиномы над изоморфным представлением поля $GF\left(16^2\right)$ не позволяют строить S-блоки по критерию максимального лавинного эффекта.

Рассмотрим пример построения S-блока конструкции Ниберг над изоморфным представлениям поля $GF(4^4)$, соответствующего критерию максимального лавинного эффекта. Пусть задан полином $f(z)=z^4+3z^3+2z^2+2$, тогда принимая во внимание (1) можем построить S-блок, таблица замены которого представляется в виде табл. 4 с шестнадцатеричным представлением элементов

Таблица 4

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	01	03	02	E4	D0	F0	49	9C	C7	B0	A0	78	50	8E	60
1	39	5A	55	CB	34	B9	D7	75	3C	68	64	77	F6	C9	30	AB
2	27	86	F5	FF	AD	56	87	20	2C	EF	67	BE	28	EE	D4	DC
3	1E	AA	4D	AF	14	B8	99	BC	5B	10	FD	4E	18	69	9A	DE
4	EA	47	E2	B4	6E	70	EB	41	F1	07	B2	7B	AE	32	3B	FC
5	0D	79	C4	D2	CA	12	25	AC	A9	84	11	38	F9	5F	F8	5D
6	0F	8F	9F	F2	1A	76	BF	2A	19	3D	BB	EC	81	94	44	71
7	45	6F	7E	C1	D6	17	65	1B	0C	51	B3	4B	B6	CD	72	C0
8	95	6C	CE	91	59	A8	21	26	D9	C3	E0	96	A3	E6	0E	61
9	CF	83	DA	E9	6D	80	8B	E1	BD	36	3E	DF	08	C6	F3	62
A	0B	B1	E7	8C	A7	FB	FA	A4	85	58	31	1F	57	24	4C	33
B	0A	A1	4A	7A	43	E3	7C	CC	35	15	ED	6A	37	98	2B	66
C	7F	73	D8	89	52	D3	9D	09	F7	1D	54	13	B7	7D	82	90
D	05	E5	53	C5	2E	DD	74	16	C2	88	92	E8	2F	D5	3F	9B
E	8A	97	42	B5	04	D1	8D	A2	DB	93	40	46	6B	BA	2D	29
F	06	48	63	9E	FE	22	1C	C8	5E	5C	A6	A5	4F	3A	F4	23

при этом таблица (табл. 5) весов производных компонентных булевых функций — $wt\left(D_{i,k}\right)$ имеет вид

Таблица 5

e_k	$wt\left(D_{1,k}\right)$	$wt\left(D_{2,k}\right)$	$wt\left(D_{3,k}\right)$	$wt\left(D_{4,k}\right)$	$wt\left(D_{5,k}\right)$	$wt\left(D_{6,k}\right)$	$wt\left(D_{7,k}\right)$	$wt\left(D_{8,k}\right)$
10000000	132	128	132	124	124	128	128	124
01000000	136	132	128	132	132	124	132	128
00100000	132	124	124	120	120	120	136	132
00010000	128	132	120	124	124	120	128	136
00001000	124	120	128	132	120	140	128	132
00000100	120	124	136	128	136	120	124	128
00000010	128	132	132	144	116	132	120	124
00000001	136	128	136	132	132	116	120	120

Как видно из анализа конструкции (табл. 5), не все компонентные булевы функции S-блока (табл. 4) достигают максимального лавинного эффекта. В соответствии с описанным методом и с учетом (3), находим множество Ψ для заданного вида S-блока (табл. 4)

$$\Psi = \{17,2B,3A,5F,66,69,AD,B5,B6,BE,D7,D9,ED,FB,\}_h . \qquad (11)$$

Поскольку выполняется неравенство $|\Psi| \geq 8$ — необходимое условие построения матрицы аффинного преобразования A, позволяющей достижение S-блоком критерия максимального лавинного эффекта выполняется.

Построим матрицу аффинного преобразования A. В нашем примере было установлено, что всего на основе множества Ψ из (11) может быть построено $|A_i| = 1073$ таких матриц и соответственно новых S-блоков удовлетворяющих критерию максимального лавинного эффекта. Например, рассмотрим одну из матриц $A = [66,B5,B6,BE,D7,D9,ED,FB]^T$. Применив данное преобразование к S-блоку (табл. 4) получим новый S-блок (табл. 6)

Таблица 6

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	F2	6F	9D	9F	B1	7E	EB	F7	3F	8F	31	68	4F	D4	3E
1	6B	3A	E2	88	2E	95	81	2D	C6	D6	61	B0	BC	15	71	B6
2	FF	3C	D3	A6	74	8D	CE	CF	78	18	0E	A5	27	EA	EE	06
3	94	44	B4	E9	E1	67	5A	38	C8	BE	3B	DB	56	24	35	9B
4	B5	C1	5D	D0	14	80	47	03	8C	30	12	07	1B	EC	F6	C9
5	45	9A	50	2C	7A	23	62	86	2B	A1	4C	99	64	97	96	0A
6	D8	26	98	E3	CB	42	57	BA	A4	34	08	77	0C	1F	AE	72
7	5C	E6	AA	FD	73	8E	93	39	B7	BD	E0	76	4D	4A	1D	0F
8	ED	89	25	B2	55	D9	3D	0D	AB	60	C0	82	5E	02	2A	CC
9	D7	91	C4	DA	7B	FE	79	32	CA	B3	5B	69	E8	CD	11	A3
A	87	7D	F0	49	01	F9	0B	6E	53	A7	83	66	7F	90	46	1E
B	75	C3	84	F5	9E	AF	37	B8	DC	13	85	4B	41	A8	48	FC
C	58	EF	59	E4	D2	DE	05	1A	4E	FB	10	D1	BF	C5	63	40
D	AD	6D	20	A2	E5	F4	DF	7C	92	16	DD	28	17	1C	A9	C7
E	8B	70	6C	22	5F	43	BB	AC	36	2F	F1	33	B9	FA	8A	D5
F	C2	19	51	6A	54	52	09	E7	65	F8	F3	9C	29	04	21	A0

Приведенный S-блок всецело соответствует критерию максимального лавинного эффекта, что подтверждается его таблицей (табл. 7) весов производных компонентных булевых функций

Таблица 7

e_k	$wt\left(D_{1,k}\right)$	$wt\left(D_{1,k}\right)$	$wt\left(D_{1,k}\right)$	$wt\left(D_{1,k}\right)$	$wt\left(D_{1,k}\right)$	$wt\left(D_{1,k}\right)$	$wt\left(D_{1,k}\right)$	$wt\left(D_{1,k}\right)$
10000000	132	132	136	128	136	132	136	144
01000000	136	132	132	132	128	132	132	132
00100000	136	144	132	144	136	132	136	136
00010000	144	136	132	132	144	136	132	132
00001000	136	132	132	136	128	136	132	136
00000100	128	128	136	132	136	144	132	132
00000010	128	132	136	136	128	136	132	132
00000001	132	128	144	132	136	128	136	132

Таким образом, можем описать предлагаемый метод построения S-блоков конструкции Ниберг с максимальным лавинным эффектом над всеми изоморфными представлениями поля $GF\left(256\right)$ в виде конкретных шагов:

Шаг 1. В соответствии с предварительно рассчитанными данными (табл. 3) выбираем вид неприводимого полинома $f(z)$. Критерием выбора конкретного вида неприводимого полинома, может быть количество подходящих матриц аффинного преобразования, приводящих к максимальному лавинному эффекту.

Шаг 2. Для выбранного на Шаге 1 неприводимого полинома с учетом (1) осуществляем построение S-блока подстановки.

Шаг 3. В соответствии с методом **M1** осуществляем синтез подходящих матриц аффинного преобразования.

Нетрудно видеть, что изменение порядка следования компонентных булевых функций из числа $8!=40320$ сохраняет критерий максимального лавинного эффекта. Каждый S-блок также может быть модифицирован $2^k=256$ способами за счет выбора вектора сдвига b, ко-

торый не влияет на матрицу весов $wt\left(D_{i,k}\right)$. Таким образом, общее число построенных S-блоков по критерию максимального лавинного эффекта определяется величиной $W = 29\,488 \cdot 8! \cdot 2^8 = 29\,488 \cdot 40320 \cdot 256 \approx 3 \cdot 10^{11}$, что является весьма привлекательным с криптографической точки зрения.

В заключении отметим основные результаты проведенных исследований:

1. Получила дальнейшее развитие теория синтеза нелинейных блоков подстановки конструкции Ниберг по критерию максимального лавинного эффекта, в рамках чего предложен метод построения S-блоков конструкции Ниберг с максимальным лавинным эффектом над всеми изоморфными представлениями поля $GF\left(256\right)$.

2. Построен полный класс объема $J = 810$ неприводимых полиномов восьмой степени над всеми изоморфными представлениями поля $GF(256)$, найдены все подходящие пары: полином – аффинное преобразование, которые обеспечивают заданные криптографические критерии качества, включая критерий максимального лавинного эффекта.

3. Предложено эффективное правило размножения S-блоков с заданными криптографическими свойствами путем $8! = 40320$ перестановок компонентных булевых функций $\left\{F_i\right\}$, $i = \overline{1,8}$, для каждого S-блока, при этом также установлено, что для каждой подходящей матрицы A аффинного преобразования вектор сдвига b может принимать $2^8 = 256$ различных структур.

4. Установлено, что объем синтезированных S-блоков конструкции Ниберг, удовлетворяющих критерию максимального лавинного эффекта составляет $W \simeq 3 \cdot 10^{11}$, что позволяет использовать эти S-блоки в качестве долговременного ключа.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Nyberg, K. Differentially uniform mappings for cryptography. In 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.
2. Chandrasekharappa, T.G.S S-boxes generated using Affine Transformation giving Maximum Avalanche Effect / T.G.S. Chandrasekharappa, K.V. Prema, Kumara Shama // Internation Journal of Computer Science and Engineering. — Manipal Institute of Technology, India. — Vol.3(#9). — 2011. — P.3185—3193.
3. FIPS 197. [Electronic resource] Advanced encryption standard. — 2001. — http://csrc.nist.gov/publications/ — 03.10.2012.
4. Берлекэмп Э. Алгебраическая теория кодирования. — М: Издательство «МИР». 1971. — с. 477.
5. Мазурков М.И. Семейства линейных рекуррентных последовательностей на основе полных множеств изоморфных полей Галуа / Мазурков М.И., Конопака Е.А // Радиоэлектроника. — 2005. — № 11. — С. 58 — 65. (Изв. вузов).