УДК 681.3.06

СОКОЛОВ А.В., БАРАБАНОВ Н.А.

АЛГОРИТМ УСТРАНЕНИЯ СПЕКТРАЛЬНОЙ ЭКВИВАЛЕНТНОСТИ КОМПОНЕНТНЫХ БУЛЕВЫХ ФУНКЦИЙ *S* -БЛОКОВ КОНСТРУКЦИИ НИБЕРГ

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

Аннотация. Исследовано явление спектральной эквивалентности компонентных булевых функций *S* -блоков подстановки конструкции Ниберг. Предложен эффективный алгоритм устранения спектральной эквивалентности, основанный на введении в каждую компонентную булеву функцию *S* -блока подстановки случайного модификатора. Анализ сгенерированных на основе предложенного алгоритма *S* -блоков подстановки подтвердил его эффективность, а также показал высокое криптографическое качество *S* -блоков подстановки.

Abstract. The phenomenon of spectral equivalence of component Boolean functions of *S* -boxes of Nyberg design is researched. An efficient algorithm to eliminate spectral equivalence based on the injection of random modifier to each component Boolean function of *S* -box is proposed. The analysis of generated based on the proposed algorithm *S* -boxes confirmed its efficiency, and also showed the high cryptographic quality of *S* -boxes.

Ключевые слова: *S* -блок подстановки, булева функция, преобразование Уолша-Адамара, спектральная эквивалентность; *S* -box, Boolean function, Walsh-Hadamard transform, spectral equivalence.

Основным примитивом, определяющим криптографические свойства современных блочных алгоритмов шифрования является *S* -блок подстановки. Задачей *S* -блока подстановки, в соответствии с принципами шифрования К. Шеннона, является конфузия, т.е. обеспечение сложной и нелинейной зависимости ключа и открытого текста [1]. Типичная конструкция современного *S* -блока подстановки состоит из дешифратора, шифратора, а также системы взаимосвязей между ними. Например, схематическое изображение *S* -блока подстановки для $k = 3$ битного входного слова показано на рис. 1.

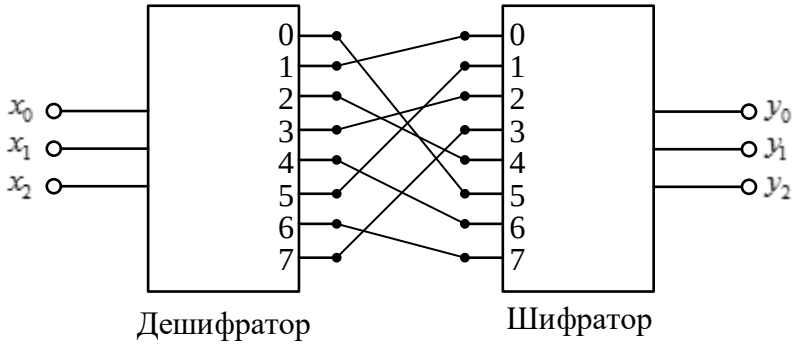

Рис. 1

Структура *S* -блока подстановки и, следовательно, его криптографические свойства могут быть полностью определены кодирующей *Q* -последовательностью длины $N = 2^k$, которая для приведенного примера имеет вид $\mathbf{Q} = \{5\ 0\ 4\ 2\ 6\ 1\ 7\ 3\}$.

В свою очередь для применения математического аппарата булевых функций для оценки криптографического качества *S* -блока подстановки кодирующая *Q* -последовательность раскладывается на множество из k компонентных булевых функций f_1, f_2, f_3, представленных в виде их таблиц истинности $\mathbf{F}^{(1)}, \mathbf{F}^{(2)}, \mathbf{F}^{(3)}$, как это для нашего примера показано в табл. 1.

Таблица 1

Q	5	0	4	2	6	1	7	3
$\mathbf{F}^{(1)}$	1	0	0	0	0	1	1	1
$\mathbf{F}^{(2)}$	0	0	0	1	1	0	1	1
$\mathbf{F}^{(3)}$	1	0	1	0	1	0	1	0

Основными критериями, предъявляемыми к современным S-блокам подстановки, являются: высокое расстояние нелинейности, в смысле расстояния до аффинного кода, низкий уровень корреляции между входными и выходными векторами данных, хороший лавинный эффект, высокие периоды возврата в исходное состояние [2]. Причем криптографическое качество S-блоков подстановки существенно растет с ростом длины N кодирующей Q-последовательности.

Задача построения S-блоков подстановки, отвечающих приведенным критериям сводится к конструированию высококачественных структур кодирующих Q-последовательностей. Тем не менее, даже для сравнительно небольших длин, количество возможных структур кодирующих Q-последовательностей стремительно растет как $J = N!$, что делает их поиск переборным методом невозможным. Так, при длине входного слова $k = 8$, применяемой в криптопреобразовании Rijndael/AES количество возможных вариантов кодирующих Q-последовательностей достигает $J = 256!$, что является астрономическим значением. Таким образом, уже для сравнительно небольших длин кодирующих Q-последовательностей построение S-блоков подстановки, обладающих высоким криптографическим качеством, является возможным только неперебoрными методами.

В криптоалгоритме Rijndael, для построения S-блока подстановки применена широко известная конструкция К.Ниберг [3], которая представляет собой мультипликативное обратное преобразование входных элементов над полем $GF(2^8)$

$$y = x^{-1} \bmod d[g(z), p], \quad y, x \in GF(2^8), \tag{1}$$

на выходе которого применяется аффинное преобразование вида

$$y' = Ay + \mathbf{a}, \quad a \in GF(2^k), \tag{2}$$

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

A — невырожденная матрица аффинного преобразования;

$\mathbf{a}$ — вектор сдвига;

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

Конструкция Ниберг характеризуется высокими значениями расстояния нелинейности, в смысле расстояния до аффинного кода, равномерной минимизацией коэффициентов корреляции векторов выхода и входа, высокой алгебраической степенью нелинейности [2]. Тем не менее, исследования [4] показывают наличие линейной избыточности, т.е. эквивалентности в компонентных булевых функциях S-блоков подстановки конструкции Ниберг, что приводит к наличию уязвимости в шифрах, использующих данную конструкцию, в том числе и в криптоалгоритме Rijndael/AES.

Целью настоящей статьи является разработка алгоритма выявления и устранения линейной зависимости между компонентными булевыми функциями S-блока подстановки конструкции Ниберг.

Обнаруженная в [4] линейная избыточность между компонентными булевыми функциями S-блока подстановки заключается в том, что все они являются аффинно-эквивалентными.

Определение 1. Две булевы функции $f(\mathbf{x})$ и $r(\mathbf{x})$ от k переменных $\mathbf{x}=\{x_0,x_1,...,x_{k-1}\}$ называются аффинно-эквивалентными если существуют не сингулярная двоичная матрица D, два k-элементных двоичных вектора $\mathbf{a}$ и $\mathbf{b}$, а также двоичная константа c, такие, что

$$r(x)=f(D\mathbf{x}^{\mathrm{T}}\oplus\mathbf{a}^{\mathrm{T}})\oplus\mathbf{b}x^{\mathrm{T}}\oplus c, \tag{3}$$

где T — оператор транспонирования.

В соответствии с Определением 1, все булевы функции группируются в неэквивалентные классы. Таким образом, для устранения линейной избыточности в S-блоках подстановки они должны строится таким образом, чтобы каждая из компонентных булевых функций $\mathbf{F}^{(1)},\mathbf{F}^{(2)},...,\mathbf{F}^{(k)}$ принадлежала различным классам аффинной эквивалентности булевых функций.

В общем случае задача аффинной классификации булевых функций является сложной. В настоящее время установлено, что для булевых функций $k=5$ переменных существует 48 классов аффинной эквивалентности [5], тогда как для булевых функций $k=6$ существует 150 357 классов аффинной эквивалентности [6].

Отметим, что сложной является не только задача полной классификации булевых функций с точки зрения аффинной эквивалентности, но также и задача определения аффинной эквивалентности двух конкретно заданных компонентных булевых функций, что усложняет задачу поиска оптимальных с точки зрения критерия отсутствия линейной избыточности структур Q-последовательностей.

В настоящей работе предлагается новый подход к определению эквивалентности компонентных булевых функций, основанный на свойствах преобразования Уолша-Адамара, который рассмотрен применительно к S-блоку подстановки конструкции Ниберг криптоалгоритма Rijndael/AES.

Пусть V_N — линейное векторное пространство бинарных векторов $\mathbf{v}^{(i)}$ длины N. Тогда полное множество $J=2^N$ элементов этого пространства в бинарном виде возможно записать как

$$V_N=\begin{Bmatrix}+&+&+&+&+&+&...&+\\+&+&+&+&+&+&...&-\\.&.&.&.&.&.&.&.\\-&-&-&-&-&-&...&-\end{Bmatrix}. \tag{4}$$

Ясно, что для каждого вектора элемента линейного векторного пространства V_N может быть поставлен в соответствие двоичный вектор длины N, представляющий собой таблицу истинности булевой функции $k=\log_2 N$ переменных путем элементарного отображения "0"$\rightarrow$"+", "1"$\rightarrow$"−".

Для каждого из векторов элементов линейного векторного пространства V_N определим преобразование Уолша-Адамара как

$$\mathbf{W}^{(i)}=\mathbf{v}^{(i)}\cdot H_N, \tag{5}$$

где H_N — матрица Адамара порядка $N=2^k$, которая строится по следующему рекуррентному правилу

$$H_{2^k}=\begin{bmatrix}H_{2^{k-1}} & H_{2^{k-1}}\\ H_{2^{k-1}} & -H_{2^{k-1}}\end{bmatrix}, \tag{6}$$

где $H_1 = 1$.

Определение 2. Элементарной структурой спектрального вектора $\mathbf{W}^{(i)}$ назовем набор абсолютных значений его спектральных компонент.

Пусть, например, задан вектор элемент линейного векторного пространства V_N $\upsilon^{(155)} = [--+--++-]$, для которого, в соответствии с (5) может быть найдено преобразование Уолша Адамара $\mathbf{W}^{(155)} = [-2\ 2\ -2\ -6\ -2\ 2\ -2\ 2]$. Так, вектор $\mathbf{W}^{(155)}$ имеет элементарную структуру $\{6(1), 2(7)\}$, где в круглых скобках указано количество раз, которое встречается приведенная спектральная компонента в спектральном векторе.

Определение 3. Две булевы функции f и r определим как спектрально неэквивалентные, если соответствующие им аффинные преобразования имеют различную элементарную структуру.

Таким образом, спектральная неэквивалентность спектров Уолша-Адамара заданных булевых функций определяется как уникальный набор абсолютных значений их спектральных компонент. В то же время, спектры эквивалентных булевых функций, содержащие один и тот-же набор абсолютных значений спектральных компонент могут быть получены друг из друга путем перестановок элементов спектра $\mathbf{W}^{(i)}$ и его знаковых кодирований, что эквивалентно некоторым аффинным преобразованиям во временной области.

В соответствии с (1) построим S-блок подстановки конструкции Ниберг, который для краткости представим в виде шестнадцатеричной таблицы подстановок

Таблица 2

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

S-блок подстановки (табл. 2) имеет расстояние нелинейности $N_S = 112$, максимальное абсолютное значение коэффициентов корреляции векторов выхода и входа $\max\{|R|\} = 0.1250$, период возврата $T = 2$.

Аналогично способу, показанному в табл. 1, S-блок подстановки (табл. 2) может быть представлен в виде $k=8$ компонентных булевых функций $\mathbf{F}^{(1)},\mathbf{F}^{(2)},...,\mathbf{F}^{(8)}$, первая из которых

$$\begin{gathered}\mathbf{F}^{(1)}=\{01101011011001110001110101101000000111011001000001001100010111111011\\ 11111011011110100011000010110011100101111111111110100000010101010010010111\\ 01000010000001010101001101000000100001111011001100110110001111010000101111\\ 00010110011101001100111001110000101010101010\},\end{gathered} \tag{7}$$

для которой найдем спектр Уолша Адамара в соответствии с формулой (5) и учетом отображения из двоичного в бинарный код

$$\begin{gathered}\mathbf{W}^{(1)}=\{0\ -12\ \ 16\ -28\ \ \ 8\ \ 12\ \ 24\ \ 12\ \ -4\ \ 24\ \ -4\ \ -8\ -12\ -16\ \ \ 4\ -16\ -24\ \ -4\ \ 24\ \ -4\ -16\ -28\ \ \ 0\ -12\\ -4\ -24\ \ 12\ -24\ \ 20\ \ 16\ -12\ \ 16\ \ -4\ -16\ \ 12\ \ 16\ \ -4\ -16\ \ -4\ \ 16\ \ \ 8\ \ \ 4\ \ \ 8\ -12\ \ \ 8\ -12\ \ \ 8\ -12\ -28\\ -24\ -12\ \ 24\ -12\ -24\ -12\ \ -8\ \ \ 8\ \ \ 4\ \ -8\ \ 20\ \ -8\ -12\ \ \ 8\ \ 20\ \ 24\ \ 12\ -16\ \ \ 4\ \ 16\ \ \ 4\ \ 24\ \ -4\ \ \ 4\ \ \ 0\\ \ -4\ \ -8\ \ 28\ \ \ 8\ \ 20\ \ 16\ \ 24\ -20\ -16\ \ 20\ \ \ 0\ \ \ 4\ -24\ -20\ -20\ \ -8\ -12\ \ 16\ -12\ \ \ 0\ \ -4\ \ \ 8\ \ \ 4\ -24\ \ 12\\ 32\ -12\ \ \ 8\ \ -4\ \ 16\ \ 16\ \ 28\ \ -8\ -12\ -16\ \ -4\ -24\ -12\ -28\ \ 24\ \ 12\ \ \ 0\ \ 20\ \ \ 8\ \ -4\ \ 32\ \ 24\ -28\ -16\ \ 28\\ -8\ -12\ \ \ 0\ \ 12\ -24\ \ 20\ \ \ 8\ \ 20\ \ 32\ \ -4\ \ \ 0\ \ 12\ \ -4\ -16\ \ -4\ -16\ \ \ 4\ \ -8\ \ 20\ \ 24\ -16\ \ 12\ \ 16\ \ -4\ \ \ 8\ \ \ 4\\ \ 8\ \ \ 4\ \ 12\ \ \ 0\ \ -4\ \ \ 0\ \ 20\ \ 24\ \ 20\ \ 24\ -12\ -16\ \ 20\ \ \ 0\ \ 20\ -16\ -28\ \ \ 0\ -24\ -20\ \ \ 8\ \ -4\ \ \ 8\ \ 28\ -24\ \ -4\\ -4\ \ 24\ \ -4\ \ 24\ \ 12\ \ 24\ \ -4\ \ -8\ \ -8\ -20\ -24\ \ -4\ -24\ \ 28\ \ -8\ \ -4\ \ \ 0\ \ 28\ -24\ \ \ 4\ \ -8\ \ 20\ -16\ \ 28\ \ \ 4\ \ \ 8\\ \ -4\ \ \ 0\ \ 28\ \ 16\ -12\ \ -8\ \ 16\ \ -4\ \ 24\ -12\ \ -8\ -12\ -16\ \ 12\ -20\ \ 16\ \ 20\ \ \ 8\ -12\ \ -8\ \ -4\ \ \ 0\ \ -4\ \ 24\ -12\\ \ \ 0\ \ -4\ \ \ 8\ \ 20\ \ 32\ -16\ -12\ \ 24\ -20\ \ \ 0\ \ \ 4\ \ 24\ \ -4\ \ 12\ -24\ \ \ 4\ \ 32\ \ 12\ \ \ 8\ -28\ \ 16\ \ 24\ -20\ \ 16\ -28\\ -24\ \ 12\ -16\ \ \ 4\}.\end{gathered} \tag{8}$$

В соответствии с Определением 2 находим элементарную структуру ξ спектрального вектора $\mathbf{W}^{(1)}$ (8)

$$\xi(\mathbf{F}^{(1)})=\{0,4,8,12,16,20,24,28,32\}. \tag{9}$$

Нетрудно показать, что и остальные компонентные булевы функции S-блока подстановки (табл.2) обладают такой-же элементарной структурой (9), а, стало быть, в соответствии с Определением 3 являются спектрально эквивалентными. Каждая из компонентных булевых функций $\mathbf{F}^{(1)},\mathbf{F}^{(2)},...,\mathbf{F}^{(8)}$ может быть получена одна из другой путем несложных преобразований спектра, таких как перестановки спектральных компонент или их знаковое кодирование, что может представлять уязвимость с точки зрения криптоанализа. Таким образом, проведенные исследования подтверждают результат [4].

В настоящей работе предложен алгоритм устранения спектральной эквивалентности компонентных булевых функций S-блока подстановки конструкции Ниберг путем введения случайного модификатора в каждую из его компонентных булевых функций. Схема введения случайного модификатора в подстановочную таблицу для длины входного вектора S-блока подстановки $k=8$ представлена на рис. 2.

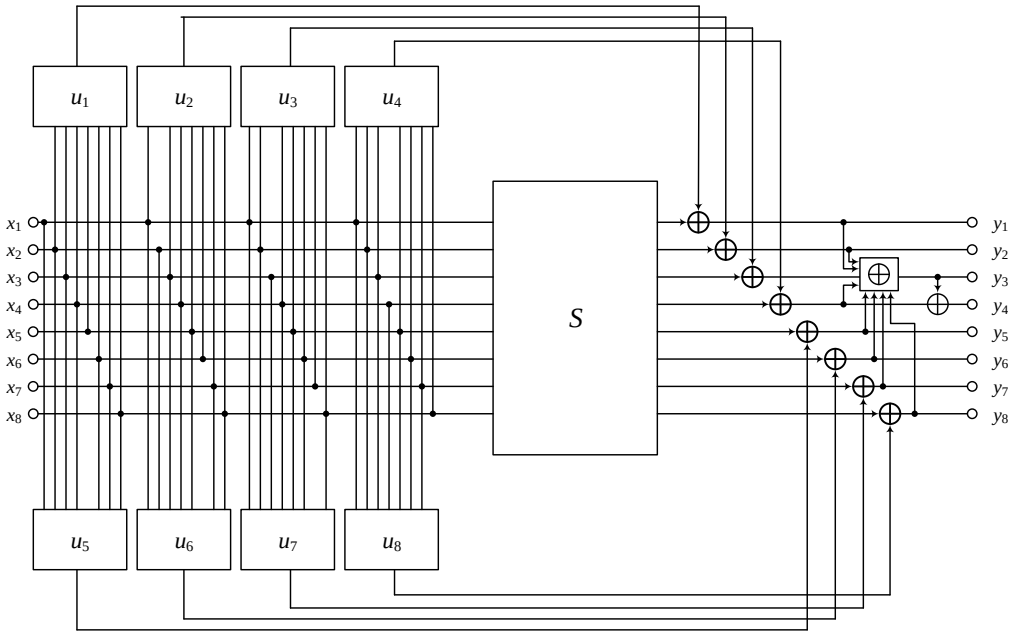

Рис. 2

В общем случае в схеме применяются в качестве случайных модификаторов 8 булевых функций $u_1, u_2, ..., u_8$ от $k-1=7$ переменных, таблицы истинности которых $\mathbf{U}^{(1)}, \mathbf{U}^{(2)}, ..., \mathbf{U}^{(8)}$ имеют длину $N = 2^{k-1} = 128$ бит. В качестве модификаторов могут применяться как высококачественные случайные последовательности [7], так и элементы ключа. Конструкция дополнительного суммирования, подключенная к 3-му выходу S-блока подстановки предназначена для сохранения его биективности, и может быть переподключена к любому из выходов S-блока подстановки.

В качестве примера работы схемы возьмем исходный S-блок подстановки (табл. 2), а также случайный модификатор

$$\begin{gathered}\mathbf{U}^{(i)} = \{11101011101000000010111000110111100110000010 \\ 11111010110001101101010000101000100010101010000111 \\ 01111101001001101011011110001101111\}, \quad i = 1, 2, ..., 8,\end{gathered} \tag{10}$$

получаем новый S-блок подстановки, представленный в табл. 3.

Таблица 3

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

Анализ построенного S-блока подстановки (табл. 3) показывает, что его компонентные булевы функции имеют 8 различных элементарных структур

$$\xi(\mathbf{F}^{(1)},\mathbf{F}^{(2)},...,\mathbf{F}^{(8)}) = \left\{ \begin{array}{l} \{0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52\} \\ \{0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 60\} \\ \{0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48\} \\ \{0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 52\} \\ \{0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 56\} \\ \{0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44\} \\ \{0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 48\} \\ \{0, 8, 16, 24, 32, 40, 48\} \end{array} \right\}. \qquad (11)$$

Построенный S-блок подстановки обладает расстоянием нелинейности $N_S = 98$, матрицей коэффициентов корреляции

$$R = \begin{bmatrix} 0 & -0.0156 & -0.0313 & -0.1875 & 0.0469 & 0 & 0.0156 & 0 \\ 0 & -0.0313 & 0 & 0.0625 & 0.0156 & -0.0625 & 0.0313 & 0.0469 \\ 0.0313 & -0.0625 & 0 & -0.0313 & 0.0625 & 0.0313 & -0.0625 & 0.0313 \\ -0.0625 & 0.1094 & -0.0938 & 0.0313 & -0.0313 & 0.0469 & -0.0313 & 0.0625 \\ -0.0313 & 0.0156 & 0.0469 & 0 & -0.1250 & -0.0938 & -0.0469 & -0.0938 \\ -0.0781 & 0.0781 & 0.0781 & -0.0313 & 0.0313 & 0.0313 & 0.0625 & 0.0781 \\ 0 & -0.0156 & 0.0313 & -0.0313 & 0.1094 & -0.0156 & 0.0156 & -0.0781 \\ -0.0469 & 0.0156 & -0.0313 & -0.0469 & 0.0469 & 0.0156 & 0.0313 & 0.0156 \end{bmatrix}, \qquad (12)$$

а также матрицей весов производных $\mathbf{D}_{i,k}$ компонентных булевых функций по направлениям $\mathbf{e}^{(j)}$ (табл. 4).

Таблица 4

$\mathbf{e}^{(j)}$	$wt\left(\mathbf{D}_{1,k}\right)$	$wt\left(\mathbf{D}_{2,k}\right)$	$wt\left(\mathbf{D}_{3,k}\right)$	$wt\left(\mathbf{D}_{4,k}\right)$	$wt\left(\mathbf{D}_{5,k}\right)$	$wt\left(\mathbf{D}_{6,k}\right)$	$wt\left(\mathbf{D}_{7,k}\right)$	$wt\left(\mathbf{D}_{8,k}\right)$
10000000	116	136	128	136	132	140	120	124
01000000	92	112	152	124	120	140	148	140
00100000	120	116	132	132	148	148	128	128
00010000	140	144	128	136	132	124	112	144
00001000	132	148	140	128	132	140	152	120
00000100	128	132	124	108	108	136	132	120
00000010	136	120	132	124	116	128	112	108
00000001	148	140	128	124	132	108	128	124

Отметим также, что построенный S-блок подстановки (табл. 3) обладает периодом возврата в исходное состояние равным $T = 9198$, что позволяет использовать его без матрицы аффинного преобразования (2). Тем не менее, аппарат аффинных преобразований может быть использован для дальнейшего наращивания периодов возврата в исходное состояние.

В заключении отметим основные результаты проведенных исследований:

1. Предложено использование спектральной эквивалентности для определения неэквивалентности компонентных булевых функций S-блоков подстановки, в рамках чего исследован S-блок подстановки конструкции Ниберг и подтверждена эквивалентность всех его компонентных булевых функций.
2. Дальнейшее развитие получил метод устранения эквивалентности компонентных булевых функций S-блока подстановки в рамках чего разработан алгоритм введения случайного модификатора в каждую из компонентных булевых функций. Предложенный алгоритм может быть легко масштабирован для любой длины k входного слова S-блока подстановки.
3. Проведенные исследования сгенерированных с помощью предложенного алгоритма S-блоков подстановки установили их соответствие основным критериям криптографического качества, что позволяет рекомендовать их к использованию в существующих криптографических алгоритмах, а также при разработке новых.

Таким образом, введение случайного модификатора является эффективным для устранения спектральной эквивалентности компонентных булевых функций S-блока подстановки при фактически полном сохранении его соответствия основным критериям криптографического качества.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Ростовцев, А.Г. Криптография и защита информации / А.Г. Ростовцев. — СПб.: Мир и Семья. — 2002.
2. Мазурков, М.И. Алгебраические свойства криптографических таблиц замен шифра Rijndael и шифра ГОСТ 28147-89 / М.И. Мазурков, А.В. Соколов. — Одесса: Труды СИЭТ. — 2012. — С.149.
3. 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 Computer Springer-Verlag. — P.55 — 65.
4. Fuller, J Linear Redundancy in S-Boxes / J. Fuller, W. Millan. — Fast Software Encryption, 10th International Workshop, Sweden, Lund, 2003. — Vol. 2887. — P. 74-86.
5. Berlekamp E.R. Weight distribution of the Cosets of the (32,6) Reed Muller Code / E.R. Berlekamp, L.R. Welch. — IEEE Transactions of Information Theory, 1972. — No. 18(1). — P. 203—207.
6. Maiorana J.A. A classification of the cosets of the Reed-Muller code r(1,6) / J.A. Maiorana. — Mathematics of Computation, 1991. — No. 57 (195). — P.403—414.
7. Мазурков, М.И. Генератор ключевых последовательностей на основе дуальных пар бент-функций / М.И. Мазурков, Н.А. Барабанов, А.В. Соколов. — Труды Одесского политехнического университета, 2013. — Вып. 3 (42). — С. 150—156.