УДК 681.3.06

СОКОЛОВ А.В.

КОНСТРУКТИВНЫЙ МЕТОД СИНТЕЗА НЕЛИНЕЙНЫХ S -БЛОКОВ ПОДСТАНОВКИ, СООТВЕТСТВУЮЩИХ СТРОГОМУ ЛАВИННОМУ КРИТЕРИЮ

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

Аннотация. Предложен конструктивный метод синтеза криптографических S -блоков подстановки, которые удовлетворяют одновременно как строгому лавинному критерию, так и критерию высокой нелинейности, причем в качестве исходного материала используются S -блоки подстановки меньшей длины и высоконелинейные бент-функции. Разработаны эффективные алгоритмы размножения полученных S -блоков подстановки.

Abstract. The constructive synthesis method of cryptographic S -boxes satisfying both the strict avalanche criterion and the criterion of high nonlinearity was introduces. Besides, as a raw material used in the method are smaller length S -boxes and nonlinear bent-functions. An effective reproduction algorithms of derived S -boxes is developed.

Ключевые слова: S -блок подстановки, строгий лавинный критерий, критерий высокой нелинейности; S -box, strict avalanche criterion, criterion of high nonlinearity.

Основными характеристиками современных блочных шифров и хэш-функций, от которых зависит уровень их защищенности, являются нелинейность и лавинный эффект. Высокое значение нелинейности шифра, ровно, как и его хороший лавинный эффект достигается за счет применения нелинейных преобразований — криптографических S -блоков подстановки, качество которых определяет защищенность криптопреобразования в целом.

S -блок подстановки — это табличная подстановка, при которой группа входных битов x_i отображается в группу выходных битов y_i в соответствии с некоторым правилом, определяемым кодирующей Q -последовательностью. Например, пусть задана кодирующая Q -последовательность длины $N=8$

$$Q=\{4\,7\,2\,6\,1\,5\,0\,3\}, \tag{1}$$

тогда структурная схема соответствующего S -блока подстановки имеет вид

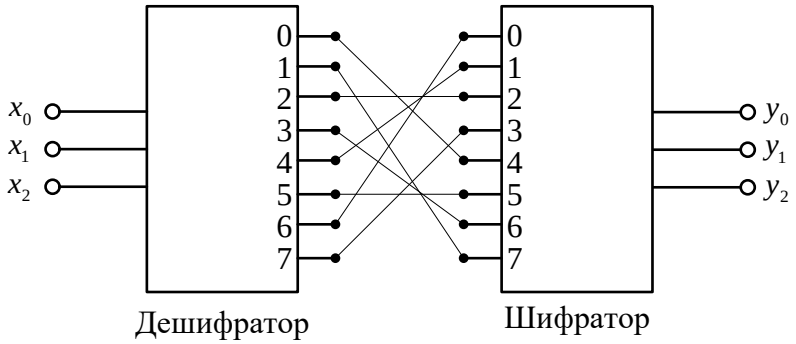

Рис.1

Каждый S -блок подстановки может быть представлен в виде $k=\log_2 N$ таблиц истинности компонентных булевых функций, например для S -блока подстановки (1) таблиц истинности $k=3$ компонентных булевых функций имеют вид

Таблица 1

Q	4	7	2	6	1	5	0	3
F_0	0	1	0	0	1	1	0	1
F_1	0	1	1	1	0	0	0	1
F_2	1	1	0	1	0	1	0	0

В качестве меры нелинейности S-блоков подстановки обычно используют расстояние нелинейности N_S в смысле максимума минимального расстояния Хэмминга от каждой его компонентной булевой функции F_i до каждой из аффинных функций [1]

$$N_S = \max\left\{\min_{i,j}\left\{dist(F_i, \varphi_j)\right\}\right\},\ i = 0,1,...,k-1,\ \ j = 0,1,...,2^{k+1}-1, \tag{2}$$

где $\varphi = \langle a, x\rangle + b$ — кодовые слова аффинного кода (кода Рида-Маллера первого порядка),

$\langle . \rangle$ — скалярное произведение по $\bmod 2$, $a, x \in V_k$, V_k — линейное векторное пространство двоичных векторов размера k, $b \in \{0,1\}$, а максимум отыскивается по всем S-блокам подстановки.

Например, можем построить все кодовые слова аффинного кода длины $N = 8$

$$\begin{cases} \varphi_0 = \{0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\}; \\ \varphi_1 = \{0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\}; \\ \varphi_2 = \{0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\}; \\ \varphi_3 = \{0\ 1\ 1\ 0\ 0\ 1\ 1\ 0\}; \\ \varphi_4 = \{0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\}; \\ \varphi_5 = \{0\ 1\ 0\ 1\ 1\ 0\ 1\ 0\}; \\ \varphi_6 = \{0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\}; \\ \varphi_7 = \{0\ 1\ 1\ 0\ 1\ 0\ 0\ 1\}; \end{cases} \quad \begin{cases} \varphi_8 = \{1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\}; \\ \varphi_9 = \{1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\}; \\ \varphi_{10} = \{1\ 1\ 0\ 0\ 1\ 1\ 0\ 0\}; \\ \varphi_{11} = \{1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\}; \\ \varphi_{12} = \{1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\}; \\ \varphi_{13} = \{1\ 0\ 1\ 0\ 0\ 1\ 0\ 1\}; \\ \varphi_{14} = \{1\ 1\ 0\ 0\ 0\ 0\ 1\ 1\}; \\ \varphi_{15} = \{1\ 0\ 0\ 1\ 0\ 1\ 1\ 0\}, \end{cases} \tag{3}$$

и в соответствии с (2) вычисляя минимум расстояния Хэмминга между каждой компонентной булевой функцией (табл. 1) и кодовыми словами аффинного кода (3) находим, что $N_s = 2$. Очевидно, бóльшее расстояние нелинейности, соответствует лучшему криптографическому качеству S-блока подстановки.

Лавинный эффект S-блока подстановки считается наилучшим, если для него выполняется строгий лавинный критерий (SAC) [2], т.е. производные каждой его компонентной булевой функции $D_{i,\nu} = F_i(x) \oplus F_i(x \oplus e_\nu)$ по всем направлениям e_ν веса $wt(e_\nu) = 1$ являются сбалансированными

$$wt\left(D_{i,\nu}\right) = 2^{k-1},\ i, \nu = 0,1,...,k-1. \tag{4}$$

Смысловая трактовка выражения (2) заключается в том, что изменение любого входного бита компонентной булевой функции F_i ведет к изменению её выходного значения с вероятностью $P = 1/2$.

Найдем, например, производные компонентных булевых функций (табл.1) S-блока подстановки (1)

$$
\begin{cases}
F_0: \\
e_0 = \{0\ 0\ 1\},\ D_{0,0} = \{1\ 0\ 0\ 0\ 1\ 1\ 1\ 0\},\ \mathrm{wt}(D_{0,0})=4; \\
e_1 = \{0\ 1\ 0\},\ D_{0,1} = \{0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\},\ \mathrm{wt}(D_{0,1})=4; \\
e_2 = \{1\ 0\ 0\},\ D_{0,2} = \{1\ 1\ 0\ 1\ 0\ 1\ 0\ 0\},\ \mathrm{wt}(D_{0,2})=4;
\end{cases}
$$

$$
\begin{cases}
F_1: \\
e_0 = \{0\ 0\ 1\},\ D_{1,0} = \{1\ 0\ 1\ 1\ 0\ 0\ 1\ 0\},\ \mathrm{wt}(D_{1,0})=4; \\
e_1 = \{0\ 1\ 0\},\ D_{1,1} = \{1\ 1\ 0\ 1\ 0\ 1\ 0\ 0\},\ \mathrm{wt}(D_{1,1})=4; \\
e_2 = \{1\ 0\ 0\},\ D_{1,2} = \{0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\},\ \mathrm{wt}(D_{1,2})=4;
\end{cases}
\qquad (5)
$$

$$
\begin{cases}
F_2: \\
e_0 = \{0\ 0\ 1\},\ D_{2,0} = \{1\ 0\ 1\ 1\ 0\ 0\ 1\ 0\},\ \mathrm{wt}(D_{2,0})=4; \\
e_1 = \{0\ 1\ 0\},\ D_{2,1} = \{1\ 1\ 0\ 1\ 0\ 1\ 0\ 0\},\ \mathrm{wt}(D_{2,1})=4; \\
e_2 = \{1\ 0\ 0\},\ D_{2,2} = \{0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\},\ \mathrm{wt}(D_{2,2})=4.
\end{cases}
$$

Таким образом, все производные компонентных булевых функций (табл. 1) по всем направлениям e_ν веса $wt(e_\nu)=1$ являются сбалансированными, стало быть, S-блок подстановки (1) удовлетворяет строгому лавинному критерию.

В последнее время исследователями достаточно много внимания уделяется конструированию S-блоков подстановки, удовлетворяющих критериям (2) или (4), однако вопрос построения S-блоков подстановки, удовлетворяющих одновременно двум критериям (2) и (4) остается нерешенным. Акцент в имеющихся разработках, в виду постоянного роста длины S-блока подстановки $N=2^k$, делается на создание регулярных методов их синтеза без применения полного перебора. Действительно, поиск подходящих S-блоков подстановки переборными методами уже при длине входного блока $k=8$, примененной в шифре Rijndael/AES, потребовал бы перебора множества, состоящего из $J=2^k!=256!$, что является технически нереализуемым.

Одним из таких конструктивных методов синтеза подстановочных конструкций, например, является конструкция Ниберг [3], применяемая в криптопреобразовании Rijndael/AES. S-блоки подстановки, построенные по правилам данной конструкции достигают практически максимального значения расстояния нелинейности $N_s=112$ [4]. Однако, оказывается, что они не соответствуют строгому лавинному критерию [5].

Попытка создания конструктивных методов синтеза S-блоков подстановки, которые бы соответствовали строгому лавинному критерию (4) предпринята в [6]. Однако, эти S-блоки подстановки не удовлетворяют критерию (2).

Целью настоящей статьи является создание конструктивного метода синтеза S-блоков подстановки удовлетворяющих одновременно строгому лавинному критерию и критерию высокого расстояния нелинейности N_S.

Для полноты изложения материала настоящей статьи приведем сущность метода построения S-блоков подстановки, соответствующих строгому лавинному критерию [6], иллюстрируя его конкретным примером:

Шаг 1. Переборным методом производится построение S-блоков подстановки, удовлетворяющих строгому лавинному критерию малой длины. Например, для длины входного блока $k=3$, такая задача не представляет трудностей, поскольку объем полного множества таких S-блоков подстановки составляет всего $J=2^k!=8!=40320$. Установлено, что для данной длины существует $V=4608$ S-блоков подстановки, удовлетворяющих строгому лавинному критерию (4). Из данного множества, выберем, к примеру, S-блок подстановки (1), обозначив его $S_k=S_3=Q$.

Шаг 2. Задается функция F_m, как MSB (старшие значащие биты) выбранного на шаге 1 S-блока подстановки S_k. В нашем случае, очевидно

$$F_m = F_2 = \{1\ 1\ 0\ 1\ 0\ 1\ 0\ 0\}. \quad (6)$$

Шаг 3. Удваивается длина функции F_m по правилу горизонтальной конкатенации

$$G_1[F_m] = \left\{F_m(x) \mid F_m\left(x \oplus e_k^{(\alpha)}\right) \oplus 1\right\},\ x = 0,1,...,2^k - 1 \quad (7)$$

где $e_k^{(\alpha)}$ — вектор длины k, содержащий 1 на позиции α; а символ "|" означает горизонтальную конкатенацию. Нетрудно видеть, что по сути $F_m\left(x \oplus e_k^{(\alpha)}\right)$ представляет собой производную функции F_m по направлению $e_k^{(\alpha)}$. Например, выберем $e_k^{(\alpha)} = \{1\ 0\ 0\}$, тогда

$$G_1[F_m] = \{0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 0\ 0\}. \quad (8)$$

Шаг 4. Удваиваем длину S-блока подстановки S_k по правилу

$$G_0[S_{k+1}] = \left\{S_k(x) \mid S_k\left(x \oplus e_t\right)\right\},\ x = 0,1,...,2^k - 1 \quad (9)$$

Для нашего примера, снова выбрав $e_k^{(\alpha)} = \{1\ 0\ 0\}$, получаем новый небиективный (т.е. такой, Q-последовательность которого содержит одинаковые элементы) S-блок подстановки

$$G_0[S_3] = \{4\ 7\ 2\ 6\ 1\ 5\ 0\ 3\ 7\ 4\ 6\ 2\ 5\ 1\ 3\ 0\}. \quad (10)$$

Шаг 5. Строим новый биективный S-блок подстановки $S_{k+1} = S_4$ удвоенной длины $N = 2^{k+1} = 16$, также соответствующий строгому лавинному критерию по правилу

$$S_{k+1} = \left\{G_1[F_m] \cdot 2^k + G_0[S_k]\right\}. \quad (11)$$

Используя полученные ранее функции $G_1[F_m]$ и $G_0[S_k]$ получаем S-блок подстановки

$$S_4 = \{4\ 7\ 2\ 14\ 1\ 13\ 8\ 11\ 15\ 12\ 6\ 10\ 5\ 9\ 3\ 0\} \quad (12)$$

Построив таблицу весов производных компонентных булевых функций $wt\left(D_{i,k}\right)$, для нового S-блока подстановки (12) удвоенной длины также получаем, что он удовлетворяет строгому лавинному критерию

Таблица 2

e_j	$wt\left(D_{1,k}\right)$	$wt\left(D_{2,k}\right)$	$wt\left(D_{3,k}\right)$	$wt\left(D_{4,k}\right)$
0001	8	8	8	8
0010	8	8	8	8
0100	8	8	8	8
1000	8	8	8	8

Шаг 6. Возвращаемся к шагу 2 и повторяем алгоритм до тех пор, пока не будет достигнут требуемая длина S-блока подстановки $N = 2^k$.

Например, повторив вышеприведенный алгоритм 5 раз получаем S-блок подстановки S_8 длины $N = 2^8 = 256$, который может использоваться в криптоалгоритме Rijndael/AES

Таблица 3

S_8	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	54	57	02	FE	01	FD	A8	AB	AF	AC	06	FA	05	F9	53	50
1	A7	A4	0E	F2	0D	F1	5B	58	5C	5F	0A	F6	09	F5	A0	A3
2	B7	B4	1E	E2	1D	E1	4B	48	4C	4F	1A	E6	19	E5	B0	B3
3	44	47	12	EE	11	ED	B8	BB	BF	BC	16	EA	15	E9	43	40
4	97	94	3E	C2	3D	C1	6B	68	6C	6F	3A	C6	39	C5	90	93
5	64	67	32	CE	31	CD	98	9B	9F	9C	36	CA	35	C9	63	60
6	74	77	22	DE	21	DD	88	8B	8F	8C	26	DA	25	D9	73	70
7	87	84	2E	D2	2D	D1	7B	78	7C	7F	2A	D6	29	D5	80	83
8	D7	D4	7E	82	7D	81	2B	28	2C	2F	7A	86	79	85	D0	D3
9	24	27	72	8E	71	8D	D8	DB	DF	DC	76	8A	75	89	23	20
A	34	37	62	9E	61	9D	C8	CB	CF	CC	66	9A	65	99	33	30
B	C7	C4	6E	92	6D	91	3B	38	3C	3F	6A	96	69	95	C0	C3
C	14	17	42	BE	41	BD	E8	EB	EF	EC	46	BA	45	B9	13	10
D	E7	E4	4E	B2	4D	B1	1B	18	1C	1F	4A	B6	49	B5	E0	E3
E	F7	F4	5E	A2	5D	A1	0B	08	0C	0F	5A	A6	59	A5	F0	F3
F	04	07	52	AE	51	AD	F8	FB	FF	FC	56	AA	55	A9	03	00

Таблица весов производных компонентных булевых функций $wt\left(D_{i,k}\right)$, для S-блока подстановки (табл. 3) также состоит из элементов равных 2^{k-1}, что говорит о том, что данный S-блок подстановки удовлетворяет строгому лавинному критерию

Таблица 4

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

Исследования свойств нелинейности S-блока подстановки (табл. 3) показали, что в соответствии с выражением (2) его расстояние нелинейности равно $N_s = 64$, что существенно меньше 112, при этом алгебраическая степень нелинейности $\deg\left(S_8\right) = 2$.

Рассмотрим возможность устранения данного недостатка, для чего более подробно изучим сущность вышеприведенного алгоритма рекуррентного увеличения длины N S-блока подстановки. Тщательный анализ данного алгоритма показывает, что по сути каждая его итерация является модификацией конструкции, показанной на рис. 2, которая была изучена в [7].

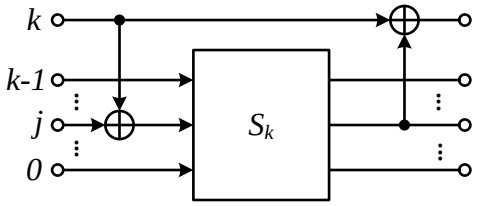

Рис. 2

Очевидно, низкая нелинейность S-блока подстановки (табл. 3) следует из недостаточно сложного закона формирования k-го выхода S-блока подстановки (рис. 2). Такое обстоятельство приводит к тому, что на каждой последующий итерации увеличения размера S-блока подстановки его нелинейность возрастает непропорционально быстро росту длины N, что ведет к неизбежной деградации данного параметра.

В данной работе установлено, что ключ к устранению указанного недостатка лежит в замене схемы, изображенной на рис. 2 на более сложную схему [7], изображенную на рис. 3, в которой применяется дополнительная булева функция g от k переменных, свойства которой будут определять сложность k-й компонентной булевой функции нового S-блока подстановки удвоенной длины.

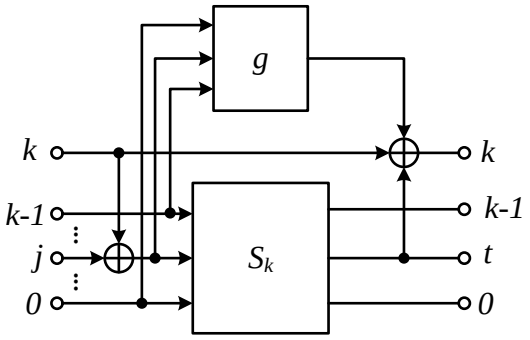

Рис. 3

Анализ работы схемы (рис. 3) показывает, что задача проектирования свойств конструируемых S-блоков подстановки может быть сведена к задаче проектирования свойств исходного S-блока подстановки S_k, а также свойств булевой функции g, применяемой на каждой итерации.

Проведенные исследования показывают, что для построения S-блоков подстановки, одновременно удовлетворяющим критериям высокой нелинейности (2) и строгого лавинного эффекта (4) в качестве исходных S-блоков подстановки S_k необходимо выбрать, такие, которые удовлетворяют строгому лавинному критерию (для малых значений k они могут быть легко найдены с помощью метода полного перебора), а в качестве функции g, длина которой на каждой итерации соответственно будет равна 2^k необходимо использовать SAC булевы функции с максимальным расстоянием нелинейности (2), для четных k, соответственно, известные в литературе как бент-функции [8].

Для таких значений $k = \{4,16,64,256...\}$, т.е. для которых $\kappa = \sqrt{k}$ является целым числом, построение необходимых для алгоритма, изображенного на рис. 3, бент-функций возможно с помощью конструкции Мэйорана МакФарланда [9] путем конкатенации строк матрицы Адамара $H(\kappa)$, их всевозможных знаковых кодирований Z и перестановок P. Всего

возможно построить $|Z|\cdot|P| = 2^k \cdot k!$ таких бент-функций. Опытным путем установлено, что все они удовлетворяют строгому лавинному критерию.

Для тех итераций алгоритма на которых $k \neq \kappa$ необходимо воспользоваться следующим утверждением:

Утверждение. На периоде бент функции Мэйорана МакФарланда длины $N = 2^\kappa$ всегда существует хотя бы один сегмент длины $\lambda = 2^k, 2 \le k \le \kappa$ удовлетворяющий строгому лавинному критерию (4).

Таким образом, мы можем записать метод построения криптографических S-блоков подстановки, соответствующих одновременно критериям (2) и (4) в виде следующих шагов, проиллюстрированных примером:

Шаг 1. Выбираем требуемый размер S-блоков подстановки $N_\tau = 2^{k_\tau}$ и исходный размер $N_u = 2^{k_u} \le N_\tau$, где индексы τ и u обозначают требуемый и исходный S-блок подстановки соответственно. Методом перебора находим все S-блоки подстановки размера N_τ соответствующие строгому лавинному критерию.

Например, пусть $N_\tau = 2^{k_\tau} = 2^8 = 256$, и исходный S-блок подстановки длины $N_u = 2^{k_u} = 2^3 = 8$ определяется (1), т.е. $S_3 = Q$.

Шаг 2. Строим булеву функцию g как двоичное отображение бент последовательности, построенной по правилу Мэйорана МакФарланда с параметрами перестановки P и знакового кодирования Z, и с учетом Утверждения. Для нашего примера в качестве такой бент-функции можно взять $g = \{0\ 1\ 1\ 0\ 1\ 1\ 1\ 1\}$.

Шаг 3. Используя схему, приведенную на рис. 3 удваиваем размер S-блока подстановки N. Если достигнут размер $N = N_\tau$ переходим к шагу 4, иначе, возвращаемся на шаг 2. В нашем примере, для достижения величины $N_\tau = 256$ потребуется совершить 5 итераций.

Шаг 4. Опытным путем установлено, что имеет место ситуация, когда нелинейность распределена по компонентным булевым функциям неравномерно, что, учитывая выражение (2) ведет к снижению общей нелинейности S-блока подстановки. Для устранения данного неравномерного распределения нелинейности по компонентным булевым функциям построенного S-блока подстановки длины $N_\tau = 2^8 = 256$ применим следующий алгоритм:

а) суммируем первую половину компонентных булевых функций по правилу

$$F_i = F_i \oplus F_6,\ i = 0,1,...,3, \tag{13}$$

б) суммируем вторую половину компонентных булевых функций по правилу

$$F_i = F_i \oplus F_3 \oplus F_7,\ i = 4,5. \tag{14}$$

Например, описанный выше алгоритм для исходного S-блока подстановки (1) и правил знакового кодирования $Z = \{1,1,...,1\}$ и перестановки $P = \{1,2,...,2^\kappa\}$, примененных на каждой итерации позволяет построить S-блок подстановки, заданной длины $N_\tau = 256$ приведенный в табл. 5.

Таблица 5

S_8	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	04	3F	1A	26	89	9D	A8	BB	01	5A	30	6C	8C	F8	82	F1
1	11	A5	7F	CC	BC	27	ED	71	14	C0	55	86	B9	42	C7	3B
2	31	35	90	93	E3	C8	7D	51	34	50	BA	D9	E6	AD	57	1B
3	24	AF	F5	79	D6	72	38	9B	21	CA	DF	33	D3	17	12	D1
4	4E	4A	5F	5C	2C	07	02	2E	FB	9F	C5	A6	99	D2	98	D4
5	5B	D0	3A	B6	19	BD	47	E4	EE	05	A0	4C	AC	68	DD	1E
6	7B	40	D5	E9	46	52	D7	C4	CE	95	4F	13	F3	87	4D	3E
7	6E	DA	B0	03	73	E8	92	0E	DB	0F	2A	F9	C6	3D	08	F4
8	FE	FA	EF	EC	9C	B7	B2	9E	4B	2F	75	16	29	62	28	64
9	EB	60	8A	06	A9	0D	F7	54	5E	B5	10	FC	1C	D8	6D	AE
A	CB	F0	65	59	F6	E2	67	74	7E	25	FF	A3	43	37	FD	8E
B	DE	6A	00	B3	C3	58	22	BE	6B	BF	9A	49	76	8D	B8	44
C	B4	8F	AA	96	39	2D	18	0B	B1	EA	80	DC	3C	48	32	41
D	A1	15	CF	7C	0C	97	5D	C1	A4	70	E5	36	09	F2	77	8B
E	81	85	20	23	53	78	CD	E1	84	E0	0A	69	56	1D	E7	AB
F	94	1F	45	C9	66	C2	88	2B	91	7A	6F	83	63	A7	A2	61

который обладает таблицей весов производных компонентных булевых функций $wt\left(D_{i,k}\right)$

Таблица 6

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

и расстоянием нелинейности $N_s = 112$, что превосходит по криптографическим свойствам S-блоки подстановки конструкции Ниберг, применяемой в криптоалгоритме Rijndael/AES.

Найдем количество различных структур S-блоков подстановки, которые могут быть построены с помощью предложенного метода. Пусть $k_u = 3$, тогда количество исходных S-блоков подстановки удовлетворяющих строгому лавинному критерию $V = 4608$, а количество бент функций Мэйорана Макфарлада $W_3 = |P||Z| = 2^4 \cdot 4! = 384$. Итого, пройдя первую итерацию мы можем построить $J_1 = 384 \cdot 4608 = 1769472$ оптимальных S-блоков подстановки. На второй итерации, из полученных S-блоков подстановки можно построить в $W = |P||Z| = 2^4 \cdot 4! = 384$ раза большее количество S-блоков подстановки, т.е. $J_2 = 384 \cdot 1769472 = 679477248$. Итого, можем записать формулу расчета мощности класса оптимальных S-блоков подстановки для k_τ-й итерации

$$J_{k_\tau} = V \cdot \prod_{k=k_u}^{k_\tau - 1} W_k \,. \qquad (15)$$

Таким образом, в соответствии с выражением (15) для $k_u = 3$, и для $k_\tau = 8$ можно построить $J_8 = (2^4 \cdot 4!) \cdot (2^4 \cdot 4!) \cdot (2^6 \cdot 6!) \cdot (2^6 \cdot 6!) \cdot (2^8 \cdot 8!) \approx 3.23 \cdot 10^{21}$ оптимальных S-блоков подстановки.

Отметим, что полученные S-блоки подстановки обладают достаточно низкими максимумами матриц коэффициентов корреляции R, при этом алгебраическая степень нелинейности сохраняется на уровне $\deg(S) = 2$, что продиктовано соответствием строгому лавинному критерию (4).

Нетрудно видеть операции, позволяющие размножение оптимальных S-блоков подстановки при сохранении их соответствия строгому лавинному критерию и критерию высокой нелинейности. Так, путем изменения порядка следования компонентных булевых функций, а также всех возможных их знаковых кодирований из одного построенного по предложенному методу S-блока подстановки могут быть построены новые $2^{k_\tau} \cdot k_\tau !$ S-блоков подстановки, большинство из которых будут также принадлежать к рассчитанному числу (15). Также новые S-блоки подстановки могут быть получены с помощью m-сдвига исходного S-блока подстановки на величину $\upsilon = 0,1,..,2^{k_\tau} - 1$ [10].

В заключении отметим основные результаты проведенных исследований:

1. Получила дальнейшее развитие теория синтеза S-блоков подстановки, соответствующих строгому лавинному критерию, в рамках чего построен метод синтеза нелинейных S-блоков подстановки оптимальных с точки зрения соответствия как строгому лавинному критерию так и критерию высокого расстояния нелинейности.
2. Установлено, что объем синтезированных оптимальных S-блоков подстановки, пригодных для использования в криптоалгоритме Rijndael равен $J_8 \approx 7.4 \cdot 10^{29}$, что является очень привлекательным с криптографической точки зрения.
3. Предложено эффективное правило размножения S-блоков подстановки с заданными криптографическими свойствами путем $k_\tau !$ перестановок и 2^{k_τ} знаковых кодирований компонентных булевых функций $\{F_i\}$, а также с помощью регулярного оператора m-сдвига.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Maier W. Nonlinearity criteria for cryptographic functions /W.Maier, O.Staffelbach // In Advances in Cryptology — EUROCRYPT’89, vol.434, Lecture Notes in Computer Science, Springer-Verlag, pp.549-562,1990.
2. Webster A.F. On the design of S-boxes / A.F. Webster, S.E. Tavares // Proc. of CRYPTO’85, Springer — Verlag. — 1985.
3. Nyberg K. Differentially uniform mappings for cryptography. I Advances in cryptology // Proceedings of EUROCRYPT’93 (1994) vol.765, Lecture Notes in Compuer Springer-Verlag, Berlin, Heidelberg, New York. P.55-65.
4. Мазурков М.И. Криптографические свойства нелинейного преобразования шифра Rijndael на базе полных классов неприводимых полиномов / М.И. Мазурков, А.В. Соколов // Труды Одесского национального политехнического университета. — №2(39). — 2012. — С.183—189.
5. Горбенко, І.Д. Дослідження аналітичних і статистичних властивостей булевих функцій криптоалгоритму RIJNDAEL (FIPS 197) / І.Д. Горбенко, О.В. Потій, Ю.А. Ізбенко // Радіотехніка: всеукр. міжвідом. наук.-техн. зб. — Харків, 2004 . — Т. 126. — С. 132 — 138.
6. Gao S. Design of bijective S-boxes satisfying the strict avalanche criterion / S. Gao, W. Ma, D. Shen // USA: Journal of computer information systems. — #6. — 2011. — P.1967—1973.
7. Kim K. A recursive construction method of S-boxes satisfying strict avalanche criterion / K. Kim, T. Matsumoto, H. Imai // Proc. of CRYPTO’90, Springer — Verlag. — 1990. — P.565—574
8. Rothaus O. On bent functions / O. Rothaus. — Alexandria, Virginia, USA: IDA CRD W.P. No. 169. — 1966.
9. McFarland R. L. A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. 1973. V. 15, N 1. P. 1 10.
10. Мазурков М.И. Алгоритм синтеза оптимальных криптографических блоков подстановки на основе регулярных операторов децимации, перестановки и m-сдвига / М.И. Мазурков, В.Я. Чечельницкий, М.А. Мельник, А.В. Соколов // Труды Одесского национального политехнического университета. — №1(38). — 2012. — С. 179—187.