УДК 681.3.06

МАЗУРКОВ М.И., СОКОЛОВ А.В.

МЕТОД СИНТЕЗА S-БЛОКОВ ПО КРИТЕРИЮ НУЛЕВОЙ КОРРЕЛЯЦИИ МЕЖДУ ВЫХОДНЫМИ И ВХОДНЫМИ ВЕКТОРАМИ ДАННЫХ И СТРОГОМУ ЛАВИННОМУ КРИТЕРИЮ

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

Аннотация. Предложен конструктивный метод синтеза корреляционно иммунных S-блоков длины $N = 256$, удовлетворяющих строгому лавинному критерию. Найдены его свойства, а также оценки количества оптимальных S-блоков, которые могут быть получены с его помощью. Предложен регулярный метод размножения полученных оптимальных S-блоков.

Abstract. The constructive synthesis method of correlation immune S-boxes of length $N = 256$ satisfying the strict avalanche criterion is proposed. Its properties, as well as the number of optimal S-boxes that can be build with it are found. The regular method of reproduction of obtained optimal S-boxes is introduced.

Ключевые слова: S-блок, корреляционный иммунитет, матрица коэффициентов корреляции, строгий лавинный критерий; S-box, correlation immunity, the matrix of correlation coefficients, the strict avalanche criterion.

Криптографический S-блок является основным компонентом практических всех современных симметричных шифров, который обуславливает его лавинный эффект, корреляционную связь векторов выхода y_j и входа x_j, а также нелинейность. Вопросы синтеза криптографически качественных S-блоков, нашли свое отражение во многих работах [1…6], где в качестве основы для их синтеза выбран тот или иной критерий. Однако для построения новых высокоскоростных криптоалгоритмов интерес представляют такие S-блоки, которые соответствуют одновременно нескольким критериям криптографического качества и таким образом позволяют эффективно противостоять одновременно нескольким видам атак криптоанализа.

Одними из наиболее существенных с практической точки зрения критериями качества S-блоков является критерий независимости векторов выхода S-блока y_j от векторов его входа x_j, известный также как корреляционный иммунитет [1], а также строгий лавинный критерий [2]. Корреляционно иммунным называется такой S-блок длины $N = 2^k$, каждая компонентная булева функция F_j, $j = \overline{1,k}$ которого обладает корреляционным иммунитетом первого или более высокого порядка $m \geq 1$, что справедливо тогда и только тогда, когда её спектральные коэффициенты Уолша-Адамара

$$W_B(\omega) = F_j \cdot A(n) = \sum_{i=0}^{n-1} F_j(i) \cdot (-1)^{\langle i,\omega \rangle} = 0\,, \quad \forall \omega, \quad wt(\omega) = m\,, \tag{1}$$

где $A(n)$ — матрица Уолша-Адамара порядка $n = N^2$, $N = 2^m$; $wt(.)$ — вес Хэмминга; $\langle i, \omega \rangle$ — скалярное произведение по $\bmod 2$ коэффициентов двоичного представления десятичных чисел, которые запишем в виде: $(i)_{10} = (i_{s-1}, i_{s-2}, \cdots, i_0)_2$ и, соответственно, $(\omega)_{10} = (\omega_{s-1}, \omega_{s-2}, \cdots, \omega_0)_2$, тогда

$$\langle i, \omega \rangle = \sum_{r=0}^{s-1} i_r \omega_r\,, \quad s = \log_2 k\,. \tag{2}$$

Если для всех компонентных булевых функций F_j, $j=\overline{1,k}$ S-блока выполняется условие (1), то он обладает идеальной (нулевой) матрицей коэффициентов корреляции векторов выхода y_j и векторов входа x_j $R=\left\| r_{\nu,\mu} \right\|$ [3], где коэффициенты корреляции

$$r_{\nu,\mu}=1-2^{-(k-1)}\sum_{z=1}^{N}\left(x_{z,\nu}\oplus y_{z,\mu}\right)=0\,,\qquad \nu,\mu=\overline{1,k}\,. \tag{3}$$

С другой стороны, строгий лавинный критерий (SAC) [2] S-блока выполняется тогда и только тогда, когда производные каждой его компонентной булевой функции $D_{j,u}=F_j(x)\oplus F_j(x\oplus e_u)$ по всем направлениям e_u веса $wt(e_u)=1$ являются сбалансированными

$$wt\left(D_{j,u}\right)=2^{k-1},\ j,u=\overline{1,k}\,, \tag{4}$$

где e_u — вектор длины k, содержащий 1 на позиции α и нулевые другие координаты.
Это фактически означает, что изменение любого входного бита компонентной булевой функции F_j приводило к изменению её выходного значения с вероятностью $P=1/2$.

В настоящие время в [1] регулярными методами синтезированы оптимальные S-блоки, соответствующие критерию (3), а также S-блоки [2], соответствующие критерию (4). Тем не менее, задача синтеза криптографических S-блоков, удовлетворяющих одновременно критериям (3) и (4) остается нерешенной, несмотря на её высокую практическую ценность.

Целью настоящей статьи является разработка метода синтеза S-блоков удовлетворяющих как критерию некоррелированности векторов выхода и векторов входа (3), так и строгому лавинному критерию (4).

Отметим, что ранее в [4] предпринималась попытка синтеза S-блоков длины $N=16$ удовлетворяющих критериям (3), (4). Переборным методом было показано, что несмотря на то, что существуют 24 булевы функции, удовлетворяющие критерию (3) и (4) на их основе не может быть построен ни один криптографический S-блок, удовлетворяющий критериям (3) и (4) одновременно.

В настоящей работе был проведен поиск булевых функций, удовлетворяющих одновременно критериям (3) и (4) длины $N=32$, в результате чего было найдено множество Ψ из 7080 сбалансированных булевых функций. Отметим, что среди данных функций нет ни одной, которая бы обладала корреляционным иммунитетом $m>1$ порядка.

Построение S-блоков на основе найденных функций переборным методом потребовало бы порядка $C_{7080}^{5}=1{,}48\cdot 10^{17}$ итераций, что является достаточно сложным с точки зрения технической реализации. Отметим, что в [5] разработан эффективный алгоритм синтеза криптографических S-блоков на основе заданного множества булевых функций, в основу которого положено предположение, что криптографический биективный (взаимнооднозначный) S-блок может быть построен только на основе таких k булевых функций для которых все линейные комбинации являются сбалансированными, т.е.

$$wt\left(\sum_{z=1}^{k}a_z\cdot\Phi_z\right)=2^{k-1},\ z=\overline{1,k}\,, \tag{5}$$

для любых $a_z\in\{0,1\}$, $\{a_1,a_2,...,a_k\}\neq\{0,0,...0\}$ и $\Phi_z=\{F_1,F_2,...,F_k\}$. При значениях $wt\left(\{a_1,a_2,...,a_k\}\right)=1$ условие (5) фактически является условием сбалансированности самих компонентных булевых функций.

Для полноты изложения материала кратко опишем Алгоритм А1 [5] построения криптографических S-блоков длины $N = 2^5 = 32$ на основе имеющегося множества булевых функций Ψ с учетом (5):

Шаг 1. Инициализируем переменные цикла $\kappa = 1$ $a = 1$.

Шаг 2. Если $a > |\Psi|$, то построение S-блоков на основе данного множества булевых функций невозможно, иначе выбираем a-ю булеву функцию из множества Ψ.

Шаг 3. Проверяем выполнение условия сбалансированности линейных комбинаций (5). Если оно выполняется, то $\kappa = \kappa + 1$, $a = a + 1$ и переходим к Шагу 4, иначе $a = a + 1$ и возвращаемся на Шаг 2.

Шаг 4. Если $\kappa < 5$ возвращаемся на шаг 2, иначе построение завершено.

Применяя данный алгоритм с различными начальными значениями a на Шаге 1 нами было построено $J = 4578$ оптимальных S-блоков длины $N = 32$, удовлетворяющих критериям (3) и (4), один из которых

$$S_5 = \{28,24,4,18,2,25,1,14,22,5,11,10,23,29,17,15,9,3,13,21,6,19,31,30,26,7,27,20,12,8,16,0\}. \quad (6)$$

Данная подстановочная конструкция обладает корреляционным иммунитетом порядка $m = 1$, и соответственно её матрица коэффициентов корреляции размера 5×5, состоящая из нулей, т.е.

$$\forall r_{\nu,\mu} = 0,\ \nu, \mu = \overline{1,5}. \quad (7)$$

Для подстановочной конструкции (6) выполняется строгий лавинный критерий (4), соответственно все компоненты таблицы весов производных равны

$$\forall wt\left(D_{j,u}\right) = 2^{k-1} = 16,\ j, u = \overline{1,5}. \quad (8)$$

Приведем распределение расстояний нелинейности N_f, а также алгебраических степеней нелинейности $\deg(F)$ [6] по компонентным булевым функциям S-блока (6)

F_j	F_1	F_2	F_3	F_4	F_5
N_F	8	8	8	8	8
$\deg(F)$	2	3	3	2	2

(9)

Тем не менее, длина построенных криптографических S-блоков, удовлетворяющие как критерию (3) так и критерию (4) является недостаточной для применения в современных криптографических алгоритмах, например Rijndael/AES [7], где $N = 2^8 = 256$.

Для увеличения длины построенных криптографических S-блоков целесообразно использовать линейный рекуррентный Алгоритм А2 [2], состоящий из следующих шагов:

Шаг 1. Задаем функцию F_m, как MSB (Most significant bit, старшие значащие биты) выбранного исходного S-блока S_k.

Шаг 3. Удваиваем длину функции F_m по правилу горизонтальной конкатенации

$$G_1\left[F_m\right] = \left\{F_m(x) \,|\, F_m\left(x \oplus e_u\right) \oplus 1\right\},\ x = \overline{0, 2^k - 1}, \quad (10)$$

где символ "|" означает горизонтальную конкатенацию.

Шаг 4. Удваиваем длину S-блока S_k по правилу

$$G_0\left[S_{k+1}\right] = \left\{S_k(x) \,|\, S_k\left(x \oplus e_t\right)\right\},\ x = \overline{0, 2^k - 1}. \quad (11)$$

Шаг 5. Строим новый биективный (взаимно-однозначный) S-блок S_{k+1} удвоенной длины $N = 2^{k+1}$ по правилу

$$S_{k+1} = \left\{ G_1\left[F_m\right] \cdot 2^k + G_0\left[S_k\right] \right\}. \tag{12}$$

Шаг 6. Возвращаемся к Шагу 1 и повторяем алгоритм до тех пор, пока не будет достигнут требуемый размер S-блока $N = 2^k = 2^8 = 256$.

Алгоритм А2 можно проиллюстрировать в виде схемы, изображенной на рис.1, где x_j — входная последовательность бит S-блока, y_j — его выходная последовательность бит.

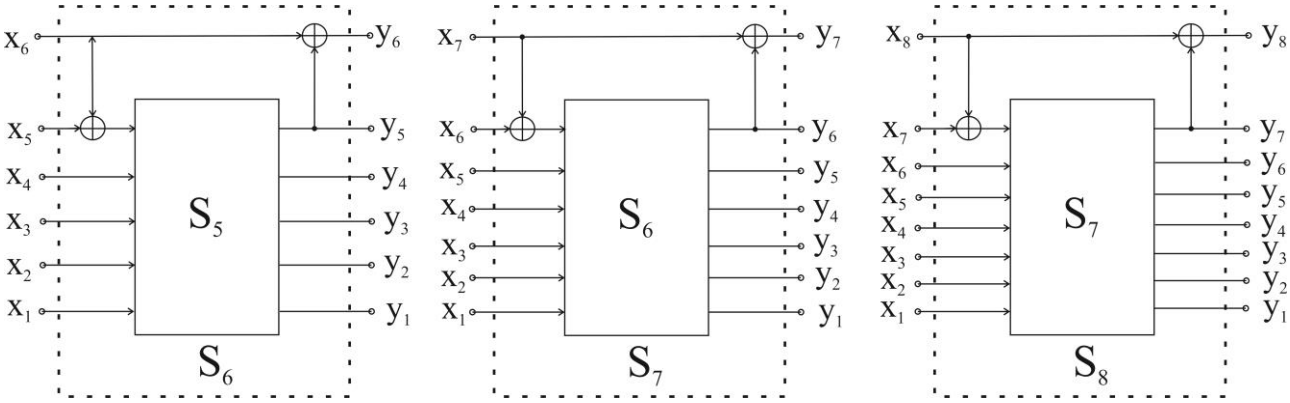

Рис. 1 — Схематическое представление алгоритма А2 рекуррентного увеличения длины S-блока

Таким образом, имея криптографический S-блок длины $N = 2^5 = 32$ в соответствии с Алгоритмом А2 можно получить криптографический S-блок длины $N = 2^8 = 256$. Причем, исследования позволили установить следующие свойства данного алгоритма:

Свойство 1. Алгоритм не изменяет исходный порядок m корреляционного иммунитета S-блока.

Свойство 2. Алгоритм не изменяет весов производных $wt\left(D_{j,u}\right)$, $j,u = \overline{1,k}$ компонентных булевых функций F_j S-блока.

Свойство 3. Алгоритм не изменяет алгебраической степени нелинейности S-блока $N_S = \min\left\{\deg\left(F_j\right)\right\}$, $j = \overline{1,k}$.

Свойство 4. На каждой итерации алгоритм удваивает расстояние нелинейности N_S S-блока.

Применяя данный алгоритм (рис.1) к S-блоку (6) получаем новый криптографический S-блок (табл. 1) длины $N = 2^8 = 256$, который в соответствии со свойствами рекуррентного алгоритма сохраняет соответствие критериям (3) и (4).

Таблица 1

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

В соответствии со Свойствами 1-4 данный S-блок обладает идеальной матрицей коэффициентов корреляции $r_{\nu,\mu}$ (3) векторов выхода y_j и векторов входа x_j, т.е.

$$\forall r_{\nu,\mu} = 0,\ \nu,\mu = \overline{1,8}.,\tag{13}$$

а также соответствует строгому лавинному критерию (4)

$$\forall wt\left(D_{j,u}\right) = 2^{k-1} = 128,\ \ j,u = \overline{1,8}.,\tag{14}$$

причем расстояния и алгебраическая степень нелинейности у данных S-блоков получаются несколько выше чем в [1] и [2].

F_j	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8
N_F	64	64	64	64	64	64	64	64
$\deg(F)$	2	3	3	2	2	2	2	2

. (15)

Таким образом, можем записать метод синтеза S-блоков, соответствующих как критерию (3) так и (4):

Шаг 1. Находим переборным методом множество булевых функций Ψ, соответствующие критериям (1) и (4).

Шаг 2. Используя Алгоритм А1 синтезируем на их основе множество S-блоков удовлетворяющих критерию (3) и (4) длины $N = 32$.

Шаг 3. Используя Алгоритм 2 проводим рекуррентное увеличение длины построенных на предыдущем шаге S-блоков до $N = 256$.

Экспериментально установлено, что применяя Алгоритм А2 можно построить $J = 4578$ криптографических S-блоков полученных в результате применения Алгоритма А1 и соответствующих критерию (3) и (4). Каждый из них состоит из компонентных булевых

функций F_j, $j=\overline{1,8}$ обладающих корреляционным иммунитетом и удовлетворяющих строгому лавинному критерию. Изменение порядка следования данных функций F_j, которое можно провести 8!=40320 способами, а также все возможные их знаковые кодирования, которых может быть $2^8=256$ комбинаций не приведут S-блок к потере криптографического качества. Таким образом, мощность класса синтезированных оптимальных S-блоков будет определятся как

$$W=4578\cdot 40320\cdot 256=4.7254\cdot 10^{10}\approx 2^{35}, \qquad (16)$$

что в принципе является достаточно существенным с криптографической точки зрения.

В заключении отметим основные результаты проведенных исследований:

— получила дальнейшее развитие теория синтеза корреляционно иммунных S-блоков, в рамках чего разработан метод синтеза S-блоков, удовлетворяющих одновременно критерию нулевой корреляции (3) векторов выхода y_j и векторов входа x_j, а также строгому лавинному критерию (4);

— установлены свойства алгоритма рекуррентного увеличения длины S-блоков, что позволило применить его для задач синтеза корреляционно иммунных S-блоков;

— показано, что несмотря на то, что для длины $N=16$ построение S-блоков, удовлетворяющих одновременно критерию нулевой корреляции выхода и входа и строгому лавинному критерию невозможно, для больших длин, уже начиная с $N=32$ такие подстановочные конструкции существуют;

— найдены эффективные методы размножения полученных оптимальных S-блоков, что позволило существенно увеличить их доступные объемы.

Таким образом, построенные высококачественные S-блоки могут быть рекомендованы для использования в современных симметричных криптографических алгоритмах, таких как Rijndael/AES для успешного противостояния атакам корреляционного и дифференциального криптоанализа.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Мазурков, М.И. Метод синтеза оптимальных подстановочных конструкций по критерию нулевой корреляции между выходными и входными векторами данных / М. И. Мазурков // Известия высших учебных заведений. Радиоэлектроника. — 2012. — Т. 55, N 12. — С. 12—22.
2. 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
3. Мазурков, М.И. Методы синтеза двоичных псевдослучайных последовательностей со свойством k-граммного распределения / М.И. Мазурков, А.В. Соколов. — Одесса: Труды ОНПУ. — 2012. — С.188 — 198.
4. Яковлєв, С.В. Збалансовані критерії якості довгострокових ключових елементів алгоритму ГОСТ 28147-89 / Яковлєв С.В. // Київ: Міжнародний науково-технічний журнал «Інформаційні технології та комп'ютерна інженерія». — 2009. — С. 5—12.
5. Kim, K. Construction of DES-like S-boxes Based on Boolean Functions Satisfying the SAC / K. Kim. — Proc. of Asiacrypt'91, Springer Verlag. — 1991. — P. 59—72.
6. 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.
7. FIPS 197. [Electronic resource] Advanced encryption standard. — 2001. — http://csrc.nist.gov/publications/ — 03.10.2012.