УДК 004.056.55

Д.Р. Григорян, Н.В. Нги

Влияние группы инерции S-блока на дифференциальную характеристику блочного шифра

Представлены результаты проверки влияния группы инерции подстановок на дифференциальную характеристику композиции линейных и нелинейных узлов, используемых в распространенных блочных шифрах. Показана зависимость, позволяющая сделать вывод о предпочтительном использовании подстановок с малой группой инерции по отношению к аффинным преобразованиям.

Ключевые слова: *S*-блок, аффинные преобразования, группа инерции, дифференциальная характеристика.
doi: 10.21293/1818-0442-2019-22-1-45-49

Нелинейность элементов, составляющих симметричные блочные криптосхемы, в большей степени влияет на стойкость подсистемы защиты информации в современных телекоммуникационных системах. Выбор качественных подстановок (*S*-блоков) считается наиболее сложной стороной разработки блочного шифра. На сегодняшний день существующий инструментарий оценки стойкости подстановок не содержит метода, определяющего наилучший *S*-блок по противодействию различным методам криптографического анализа и способам их аппаратной и/или программной реализации [1, 2].

В современных алгоритмах (AES, «Кузнечик») вместо фиксированных перестановок применяются линейные отображения, изменяющие установленный *S*-блок (часто единственный) на другой из достаточно большого множества ему эквивалентных.

В данной работе предпринята попытка определения подстановки (*S*-блока), которая в соответствующих шифрах даст минимальное значение дифференциальной характеристики.

Аффинно-эквивалентное преобразование *S*-блока

Сначала необходимо ответить на вопрос, как много можно получить *S*-блоков, аффинно-эквивалентных заданному? Рассмотрим *S*-блок, полученный путем обращения элементов векторного пространства V_4 по модулю примитивного полинома $h(x)$ четвертой степени, аналогично методике, описанной в [2], и запишем его в табл. 1.

Таблица 1

Пример представления *S*-блока

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	1	9	E	D	B	7	6	F	2	C	5	A	4	3	8

Аффинно-эквивалентными (Affine General Linear Group, AGL) будут все подстановки, полученные из заданной R_0 (назовем ее представитель) в соответствии с выражением (1):

$$S = \mathbf{B} \cdot R_0(\mathbf{A} \cdot x \oplus \mathbf{a}) \oplus \mathbf{b}, \qquad (1)$$

где **A** и **B** – невырожденные матрицы размером $n \times n$, **a**, **b** – n-мерные векторы [4].

Сгруппировав *S*-блоки, получаемые из R_0 аффинно-эквивалентным преобразованием по значениям матрицы **A** и вектора **a**, формируется модель процесса генерации множества *S*-блоков относительно аффинной эквивалентности (рис. 1).

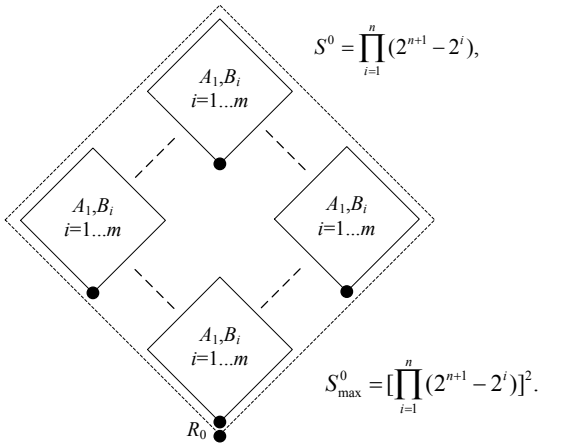

Рис. 1. Модель процесса генерации множества *S*-блоков относительно аффинной эквивалентности

На рис. 1 все множество аффинно-эквивалентных *S*-блоков S^0 показано пунктирной линией. Ромбами внутри показаны подмножества *S*-блоков, имеющие при получении из R_0 одинаковые матрицы $\mathbf{A}_1$, векторы a и все возможные значения матрицы $\mathbf{B}_j$ и векторы **b**. То есть смежные классы аффинно-эквивалентных подстановок. Точки внизу ромбов – минимальные представители данных подмножеств или локальные представители данного смежного класса. Точка внизу рисунка – искомый представитель R_0 всего множества [5, 6].

Как и в [4], *S*-блок, имеющий n входов, представляется в виде таблиц истинности составляющих его координатных булевых функций [7]. Основным отличием является подход к взвешиванию *S*-блоков: в данном случае таблица истинности, формирующая *S*-блок, рассматривается по столбцам, т.е. как n цифр системы счисления с основанием $M = 2^{2^n}$. Младший разряд этого числа определяется первой координатной функцией, старший n-й. Таким образом, представителем R_0 всего множества аффинно-эквивалентных *S*-блоков является тот, у которого минимальное значение веса. Локальным представи-

телем является *S*-блок, обладающий наименьшим весом из всех *S*-блоков, полученных при всех возможных значениях матрицы **B** и вектора **b**, при фиксированных значениях матрицы **A** и вектора **a**.

Определение числа представителей

Для фиксированных матриц **A** и векторов **a**, путем перебора значений **B** и **b** ищется представитель с наименьшим весом. Количество *различных* представителей из всех полученных предлагается использовать в качестве показателя оценки качества *S*-блока. Обозначим это число N_{lm}, соответствующее числу представителей (локальных минимумов). Возможное количество подмножеств множества аффинно-эквивалентных *S*-блоков, а следовательно и представителей, не может превышать границу (2):

$$N_{\text{lm}} \le \prod_{i=1}^{n} (2^{n+1} - 2^i) . \qquad (2)$$

Максимально возможное число представителей для различных значений n представлено в табл. 2.

Таблица 2

Максимальное число представителей

n	$\max N_{lm}$
4	322560
5	319979520
6	1290157424640
7	20972799094947840
8	1369104324918194995200
16	2,191516442724341427197177313e+81

В качестве критерия оценки качества *S*-блоков предлагается использовать количество получаемых локальных представителей [8]. Так, множество аффинно-эквивалентных *S*-блоков, построенное для блока подстановки с размерностью n = 4, использованного в алгоритме «Магма», имеет существенно больше локальных представителей, чем *S*-блок такой же размерности, полученный путем обращения. Результаты экспериментов для различных аффинно-неэквивалентных *S*-блоков представлены в табл. 3. Под нелинейностью N_{Sbox} здесь и далее понимается наименьшее расстояние Хемминга координатных функций *S*-блока и их линейных комбинаций, от всех аффинных. Существенно нелинейными будем считать *S*-блоки, содержащие функции с нелинейностью, близкой к нелинейности бэнт-функций [3].

Таблица 3

Аффинно-неэквивалентные *S*-блоки 4×4

S-блок	N_{Sbox}	N_{lm}
D2781EB45AF093C	0	1
0FA5C369872D4BE1	0	1
01C86F4E3DBA2975	2	5376
019EDB76F2C5A438(*inv*)	4	5376
0123468A5BCF7E9D	4	80640
C462A5B9E8D703F1(ГОСТ)	4	322560

Тот факт, что *S*-блоки, имеющие одинаковые показатели нелинейности, могут иметь значительно отличающиеся характеристики по другим показателям, например, количеству локальных представителей, позволяет сделать вывод, что значение нелинейности для *S*-блоков не может считаться исчерпывающим показателем качества [9].

На основе выработанного показателя можно определить мощность множества S^0 аффинно-эквивалентных *S*-блоков, полученных: из исходного линейного (на рис. 1 верхнее выражение) и *S*-блока, обладающего существенной нелинейностью (нижнее выражение).

Кроме того, можно оценить количество смежных классов N_{lm} во множестве S^0 и путем сравнения полученной оценки с ее максимальным значением max N_{lm}, представленным в табл. 3, и сделать вывод о качестве *S*-блока. Чем меньше полученная разница, тем лучше *S*-блок.

Определение 1. Коэффициентом использования множества подстановок (тела инерции) $k_{\text{ти}}$ назовем отношение

$$k_{\text{ти}} = \frac{N_{\text{lm}}}{\max N_{\text{lm}}} . \qquad (3)$$

Очевидно, что при $k_{\text{ти}} = 1$ группа инерции соответствующей подстановки по отношению к аффинно-эквивалентным преобразованиям тривиальна (равна 1) [10].

Влияние характеристик *S*-блока на значение дифференциальной характеристики блочного шифра

Разности $\Delta x, \Delta y$ над F_2 называют дифференциалом подстановки, а x, y – двоичные последовательности наборов входа и выхода подстановки.

Допустим, x, x' – наборы входа подстановки и y, y' – соответствующие наборы выхода [11]. Тогда матрицу дифференциалов подстановок составляют для удобства числовыми разностями. Разностный вектор $\Delta\mathbf{x} = a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus a_4x_4$ представляют в виде числа $\mathbf{a} = 8a_1 + 4a_2 + 2a_3 + a_4$. Общее количество разностных выражений – 16, каждому из которых соответствует 16 пар входных наборов x, x'. Таким же образом задают разностный вектор $\Delta\mathbf{y} = b_1y_1 \oplus b_2y_2 \oplus b_3y_3 \oplus b_4y_4$ соответствующим числом $\mathbf{b} = 8b_1 + 4b_2 + 2b_3 + b_4$ [12].

Допустим, входной набор x для разности **a** может принимать 16 значений. Для каждого x и соответствующего x' вычислим результаты подстановки и соответствующее разностное значение **b**. Элемент c_{ab} разностной матрицы определяется числом встречаемости выходного разностного значения **b** для входного дифференциала **a**. Матрица разностных значений в полной мере задает как дифференциалы *S*-блока, так и частоту их появления (табл. 4).

Благодаря вычисленной таблице дифференциалов, легко определяются одноцикловые дифференциалы криптографического преобразования и их вероятности [13].

Определение 2. i-цикловым дифференциалом шифрования являются два вектора $[\boldsymbol{\alpha},\boldsymbol{\beta}]_i$, такие, что открытые наборы текстов x, x' с разностью α спо-

собны быть преобразованы после *i*-й итерации в выходной набор текстов y, y' с разностью β.

Таблица 4

Разностная матрица для *S*-блока из табл. 1

Разницы входов, представленные числами (*a*)	Разницы выходов, представленные числами (*b*)									
	0	1	2	3	…	C	D	E	F
0	16	0	0	0	…	0	0	0	0
1	0	0	2	2	…	0	2	2	2
2	0	2	2	2	…	0	0	4	0
3	0	2	2	2	…	0	4	0	0
4	0	2	2	0	…	2	2	0	0
5	0	0	0	0	…	2	2	2	4
6	0	2	0	0	…	4	0	0	0
7	0	0	0	2	…	0	2	4	2
8	0	0	2	0	…	0	0	0	2
9	0	2	0	0	…	0	0	2	0
A	0	2	0	2	…	0	0	0	2
B	0	0	0	0	…	0	2	0	2
C	0	0	0	2	…	2	2	0	0
D	0	0	2	0	…	2	0	2	0
E	0	4	2	2	…	0	0	0	0
F	0	0	2	2	…	4	0	0	2

Определение 3. Вероятность дифференциала *i*-го цикла для векторной пары $[\boldsymbol{\alpha},\boldsymbol{\beta}]_i$ – это условная вероятность равенства β разности $\Delta y(i)$ двух выходных текстов y, y' после *i*-го цикла при условии, что Δx соответствующих входных наборов равна α, когда входные x или x' и раундовые ключи взаимно независимы и равновероятны [3]:

$$P(\Delta y(i) = \beta \mid \Delta x = \alpha). \qquad (4)$$

Совместно с определением дифференциала *i*-го цикла известно понятие дифференциальной характеристики.

Определение 4. Дифференциальной характеристикой называют множество одноцикловых дифференциалов, в котором выходной дифференциал векторов одного цикла совпадает с входным дифференциалом следующего.

Рассмотрим влияние параметров *S*-блока на значение дифференциальной характеристики композиции линейных и нелинейных отображений (*S*-блок, *L*-преобразования) [15], основная идея которого состоит в вычислении среднего ее значения для всех полученных аффинно-эквивалентных блоков и представлена на рис. 2.

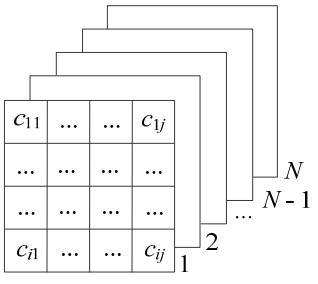

Рис. 2. Модель представления таблиц распределения дифференциалов для аффинно-эквивалентных *S*-блоков

При проведении опытов будем изменять только матрицы **A** и **B**, поскольку роль векторов **a** и **b** будут играть соответствующие раундовые ключи.

Исследование дифференциальной характеристики существенно нелинейных *S*-блоков

На рис. 3 приведены результаты суммирования таблиц распределения дифференциалов для *S*-блока, полученного путем обращения, у которого наибольший дифференциал составляет 4 [14]. Уже за пятьсот итераций алгоритма анализируемые параметры (max, min, Δ, т.е. максимальное, минимальное значения полученных средних значений и разность между ними) приближаются к ≈ 1,3; 0,8 и 0,5 соответственно. Такие значения существенно меньше исходных и с увеличением числа итераций уменьшаются, но не так интенсивно, как в начале алгоритма.

Следующим этапом является применение разработанного алгоритма к *S*-блоку из отечественного ГОСТа «Магма». Итоги экспериментов представлены на рис. 4.

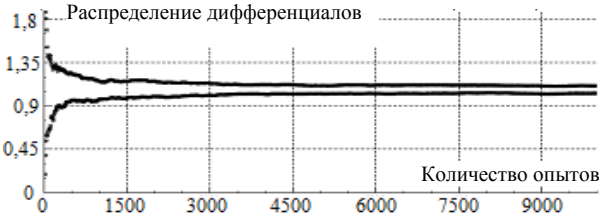

Рис. 3. Дифференциальная характеристика *S*-блока, полученного путем обращения

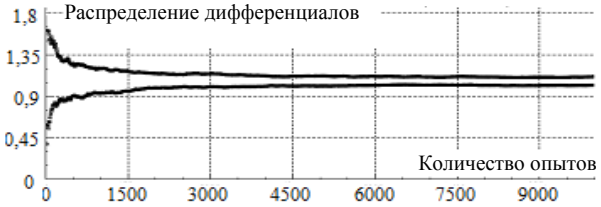

Рис. 4. Дифференциальная характеристика *S*-блока «Магма»

Оценка значения максимального дифференциала *S*-блоков больших размерностей при их совместном использовании с линейными отображениями

Для начала составим таблицу распределения дифференциалов. Для *S*-блока, полученного путем обращения (типа AES), максимальная частость дифференциала равна 4, минимальная – 0. Ниже в табл. 5 представлены результаты опытов.

Далее рассмотрим результаты, полученные для *S*-блока, использующегося в алгоритме «Кузнечик» (табл. 6). По сравнению с американским аналогом стойкость с точки зрения дифференциального криптоанализа должна быть ниже.

Для наглядности дифференциальные характеристики композиций (*S*-блок, *L*-преобразования) представлены в табл. 7.

Таблица 5

Результаты экспериментов для *S*-блоков типа AES

S-блок	N_{sbox}	max	min	Δ	Кол-во опытов
AES	112	1,3	0,7	0,6	100
		1,2	0,84	0,36	300
		1,16	0,85	0,31	500
		1,14	0,88	0,26	700
		1,12	0,89	0,23	1000

Таблица 6

Результаты экспериментов для *S*-блока «Кузнечик»

S-блок	N_{sbox}	max	min	Δ	Кол-во опытов
ГОСТ	100	1,34	0,6	0,74	100
		1,27	0,72	0,55	300
		1,21	0,79	0,42	500
		1,17	0,81	0,36	700
		1,15	0,86	0,29	1000

Таблица 7

Сравнение характеристик *S*-блоков «Кузнечик» и AES

		Количество опытов					
		1	100	300	600	900	1000
ГОСТ	max	8	1,3	1,25	1,2	1,16	1,15
	min	0	0,6	0,71	0,81	0,85	0,86
AES	max	4	1,3	1,2	1,15	1,12	1,12
	min	0	0,7	0,84	0,86	0,88	0,9

Из сравнения видно, что значение максимального дифференциала довольно быстро снижается. Сравнивая результаты с *S*-блоком размерности $n = 4$, можно увидеть, что исследуемые показатели у *S*-блоков с $n = 8$ уменьшаются даже быстрее. Кроме того, несмотря на то, что исходная дифференциальная характеристика *S*-блока из алгоритма «Кузнечик» в два раза хуже, чем у *S*-блока AES, для обоих блоков замены за 100 итераций они практически равны. Данный факт объясняется тем, что группа инерции у *S*-блока «Кузнечик» тривиальна. В то время, как для *S*-блока AES, она равна $\cong 1 \cdot 10^{13}$.

Выводы

Таким образом, при построении блочных шифров необходимо использовать *S*-блоки с минимальной группой инерции ($k_{\text{ти}} = 1$) и линейные узлы, которые способны обеспечить выбор преобразования, близкий к равновероятному.

Несмотря на то, что с увеличением размера подстановки доля подстановок с тривиальной группой инерции растет, задача определения группы инерции для конкретной подстановки не тривиальна. Поэтому направлением дальнейших исследований можно считать, разработку эффективных алгоритмов оценки значения группы инерции подстановок по отношению к аффинным преобразованиям.

Литература

1. Панасенко С.П. Алгоритмы шифрования: специальный справочник. – БХВ-Петербург, 2009. – 576 с.

2. Зензин О.С. Стандарт криптографической защиты – AES. Конечные поля / О.С. Зензин, М.А. Иванов. – М.: КУДИЦ-ОБРАЗ, 2002. – 176 с.

3. Логачев О.А. Булевы функции в теории кодирования и криптологии / О.А. Логачев, А.А. Сальников, С.В. Смышляев. – М.: ЛЕНАНД, 2015. – 576 с.

4. Birykov A. A Toolbox for Cryptanalysis: Linear and Affine Equi-valent Algorithms / A. Birykov, C. De Cannere, A. Braeken, B. Prenell // Advances in Cryptology: EUROCRYPTO–2003. – Springer, 2003. – Vol. 2656. – P. 33–50.

5. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях: пособие. – М.: ДМК-Пресс, 2012. – 592 с.

6. Изотов Б.В. Модели управляемых подстановочных операций и синтез блочных алгоритмов защиты информации: автореф. дис. … канд. техн. наук. – СПб., 2001. – С. 22–24.

7. Wei Guo Z. Constructions of almost optimal resilient Boolean functions on large even number of variables / Z. Wei Guo, X. Guo Zhen // Information Theory IEEE Transactions on. – 2009. – P. 5822–5831.

8. Luật 51/2005/QH11 Giao dịch điện tử Việtnam. – 2005.

9. 170/2013/NĐ-CP Hướng dẫn Luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số. – 2013.

10. Харин Ю.С. Математические основы криптографии / Ю.С. Харин, В.И. Бердник, Г.В. Матвеев. – Минск: БГУ, 1999. – 319 с.

11. Яшенко В.В. Введение в криптографию. – М.: МЦМНО, 2000. – 288 с.

12. Ростовцев Г.А. Алгебраические основы криптографии. – СПб.: НПО «Мир и семья», ООО «Интерлайн», 2000. – 354 с.

13. Чмора Л.А. Современная прикладная криптография. – М.: Гелиос АРИ, 2001. – 256 с.

14. Construction of highly nonlinear resilient S-boxes with given degree / F.U. Shaojing et al. // Designs, Codes and Cryptography. – 2012. – P. 241–253.

15. Lisitskaya I.V. Importance of S-Blocks in Modern Block Ciphers / I.V. Lisitskaya, E.D. Melnychuk, K.E. Lisitskiy // International Journal of Computer Network & Information Security. – 2012. – P. 4–10.

Григорян Даниил Рубенович
Сотрудник Академии федеральной службы охраны (ФСО) России
Приборостроительная ул., 35, г. Орёл, Россия, 302034
Тел.: +7 (486-2) 54-99-33
Эл. почта: daniil96grigoryan@yandex.ru

Нги Нгуен Ван
Адъюнкт Академии ФСО России
Приборостроительная ул., 35, г. Орёл, Россия, 302034
Тел.: +7-920-819-68-41
Эл. почта: nghinv25@gmail.com

Grigoryan D.R., Nghi N.V.

Influence of inertia group of the *S*-box on the differential characteristic of the box cipher

The article presents the testing results for various groups and substitutions on the differential characteristics of compositions of linear and nonlinear nodes in common box ciphers. A relationship is shown that allows prioritizing the use of

substitutions with a small group of inertia to the one of affine transformations.

Keywords: *S*-box, affine transformations, inertia group, differential characteristic.
doi: 10.21293/1818-0442-2019-22-1-45-49

References

1. Panasenko S. P. *Algoritmj shivrovanija. Specialnij spravochnik* [Encryption algorithms. Special reference].Saint-Petersburg, BHV-Petersburg, 2009. 576 p.

2. Zenzin O.S, Ivanov M.A. *Standart criptographicheskoy zashitj AES. Konechnie polja* [Cryptographic protection standard – AES. Finite field]. M., KUDIC-OBRAZ, 2002. 176 p.

3. Logachev O.A., Salnikov A.A., Smjshlyaev S.V. *Bulevj funkzii d teorii kodirovanija I cryptologii* [Boolean functions in coding theory and cryptology]. M., LENAND, 2015. 576 p.

4. A. Birykov, Christophe De Cannere, A. Braeken, B. Prenell. A Toolbox for Cryptanalysis: Linear and Affine Equivalent Algorithms. *Advances in Cryptology: EUROCRYPTO–2003*, 2003, vol. 2656, pp. 33–50.

5. Shangin V.F. *Zashita informacii d computernjh sistemah I setjah. Rukovodstvo* [Protection of information in computer systems and networks. Guide book]. M., DMK-Press, 2012, 592 p.

6. Izotov B. V. *Modeli upravljameh podstanovochnjh operazii i sintez blochnjh algoritmov zashitj informazii* [Models of controlled substitution operations and synthesis of block algorithms of information security. Cand. Diss. Abstract]. SPb., 2001. pp. 22–24.

7. Wei Guo Z., Guo Zhen X. Constructions of almost optimal resilient Boolean functions on large even number of variables. *Information Theory, IEEE Transactions on*, 2009, pp. 5822–5831.

8. Luật 51/2005/QH11 Giao dịch điện tử Việt Nam. 2005.

9. 170/2013/NĐ-CP Hướng dẫn Luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số. 2013.

10. Harin U.S., Berdnik V.I., Matveev G.V. *Matematicheskie osnovj cryptographii* [Mathematical foundations of cryptography]. Minsk, BGU, 1999. 319 p.

11. Jaschenko V.V. *Vvedenie v cryptographij* [Introduction to cryptography]. M., MZMNO, 2000. 288 p.

12. Rostovzev G.A. *Algebraicheskie osnovj cryptographii* [Algebraic the basics of cryptography]. SPb., NPO «Mir i semja», OOO «Interlain», 2000. 354 p.

13. Chmora L.A. *Sovremennaja prikladnaja cryptographija* [Modern applied cryptography]. M., Gelios ARI, 2001. 256 p.

14. Shaojing FU, et al. Construction of highly nonlinear resilient S-boxes with given degree. *Designs, Codes and Cryptography*, 2012, pp. 241–253.

15. Lisitskaya I.V., Melnychuk E.D., Lisitskiy K.E. Importance of S-Blocks in Modern Block Ciphers. *International Journal of Computer Network & Information Security*. 2012, pp. 4–10.

Daniil R. Grigoryan
Employee, Academy of Federal Guard Service of Russia
35, Priborostroitel`naya st., Oryol, Russia, 302034
Phone: +7 (486-2) 54-99-33
Email: daniil96grigoryan@yandex.ru

Nguen Van Nghi
Adjunct, Academy of Federal Guard Service of Russia
35, Priborostroitel`naya st., Oryol, Russia, 302034
Phone: +7-920-819-68-41
Email: nghinv25@gmail.com