S-блоки: определения, примеры.

S-блоки (блок подстановок, s-box, substitution box) являются одним из основных компонентов, определяющих нелинейность шифрующего преобразования и уровень стойкости современных симметричных криптографических алгоритмов. При проектировании многих симметричных блочных алгоритмов шифрования S-блоки часто выбирают с целью реализации конфузии в шифре. Тем самым криптостойкость шифров сильно зависит от криптографических свойств S-блоков. S-блоки представляют собой подстановки, которые отображают n-битовый входной блок в выходной длиной m бит.

Математически S-блоки определяются с помощью булевых функций и векторных булевых функций.

Как известно, булевой функцией (от n переменных) называется отображение $f : B^n \to B$, где $B = GF(2)$ конечное поле порядка 2.

Одним из основных способов представления булевой функции $f : B^n \to B$ является таблица истинности, т.е. таблица следующего вида

x_1	x_2	...	x_{n-1}	x_n	$f(x_1,x_2, ...,x_{n-1},x_n)$
0	0	...	0	0	f(0,0,...,0,0)
0	0	...	0	1	f(0,0,...,0,1)
0	0	...	1	0	f(0,0,...,1,0)
0	0	...	1	1	f(0,0,...,1,1)
...	...	...	...	...	...
1	1	...	0	0	f(1,1,...,0,0)
1	1	...	0	1	f(1,1,...,0,1)
1	1	...	1	0	f(1,1,...,1,0)
1	1	...	1	1	f(1,1,...,1,1)

Замечание. Наборы значений переменных в таблице записаны в таком порядке, чтобы строки цифр $x_1x_2...x_{n-1}x_n$, рассмотренные как двоичные числа, были упорядочены по возрастанию.

Также имеет значение количество так называемых существенных переменных.

Переменная x_i называется существенной переменной функции $f(x_1, x_2, ..., x_n) : B^n \to B$, если существуют такие $a_1, a_2, .., a_{i-1}, a_{i+1}, .., a_n \in B$, что $f(a_1, a_2, .., a_{i-1}, 0, a_{i+1}, .., a_n) \neq f(a_1, a_2, .., a_{i-1}, 1, a_{i+1}, .., a_n)$. В противном случае переменная x_i называется фиктивной.

Альтернативным табличным представлением булевой функции $f : B^n \to B$ является таблица следующего вида:

x_1	x_2	...	x_{n-1}	x_n	$f(x_1,x_2, ...,x_{n-1},x_n)$
0	0	...	0	0	$(-1)^{f(0,0,...,0,0)}$
0	0	...	0	1	$(-1)^{f(0,0,...,0,1)}$
0	0	...	1	0	$(-1)^{f(0,0,...,1,0)}$
0	0	...	1	1	$(-1)^{f(0,0,...,1,1)}$
...	...	...	...	...	...
1	1	...	0	0	$(-1)^{f(1,1,...,0,0)}$
1	1	...	0	1	$(-1)^{f(1,1,...,0,1)}$
1	1	...	1	0	$(-1)^{f(1,1,...,1,0)}$
1	1	...	1	1	$(-1)^{f(1,1,...,1,1)}$

Другим важным способом представления булевой функции $f : B^n \to B$ является алгебраическая нормальная форма функции, т.е. представляющий ее многочлен от n переменных над полем B вида

$$f(x_1, x_2, .., x_n) = a \oplus a_1 x_1 \oplus a_2 x_2 \oplus .. \oplus a_n x_n \oplus a_{12} x_1 x_2 \oplus a_{13} x_1 x_3 \oplus .. \oplus a_{12..n} x_1 x_2 ... x_n ,$$

где $a, a_1, a_2, .. a_n, a_{12}, a_{13}, .., a_{12..n} \in B$.

Замечание. Другое известное название алгебраической нормальной формы булевой функции - полином Жегалкина.

В случае представления булевой функции с помощью алгебраической нормальной формы важной характеристикой является алгебраическая степень $\deg(f)$ булевой функции $f: B^n \to B$, т.е. число переменных в самом длинном слагаемом её алгебраической нормальной формы. Тогда можно выделить аффинные, квадратичные и кубические булевы функции. Аффинной булевой функцией называется функция с алгебраической степенью, равной 1 (в случае, когда $a = 0$ линейной). Квадратичной булевой функцией называется функция с алгебраической степенью, равной 2. Кубической булевой функцией называется функция с алгебраической степенью, равной 3.

Еще большое значение для представления булевой функции имеют преобразование Фурье и преобразование Уолша.

Преобразованием Фурье булевой функции $f: B^n \to B$ называется функция $\underline{W_f}: B^n \to Z$, определяемая равенством $\underline{W}_f(u) = \sum_{x \in B^n} (-1)^{(x,u)} f(x)$. Значение $\underline{W}_f(u)$ для каждого $u \in B^n$ называется коэффициентом Фурье.

Преобразованием Уолша булевой функции $f: B^n \to B$ называется функция $W_f: B^n \to Z$, определяемая равенством $W_f(u) = \sum_{x \in B^n} (-1)^{(x,u)} (-1)^{f(x)}$. Значение $W_f(u)$ для каждого $u \in B^n$ называется коэффициентом Уолша.

Таблица истинности, алгебраическая нормальная форма, преобразования Фурье и Уолша однозначным образом определяют булеву функцию. Еще одна форма представления булевой функции – это ее автокорреляционная функция. Однако она не определяет булеву функцию однозначно.

Как было указано выше, математически S-блок также определяется с помощью векторных булевых функций.

S-блоком (блоком подстановок) называется векторная булева функция $F: B^n \to B^m$, где B - конечное поле порядка 2.

Существуют различные способы представления S-блоков такие, как таблица истинности, алгебраическая нормальная форма, преобразование Фурье, преобразование Уолша, автокорреляционная функция. Также S-блок $F: B^n \to B^m$ может быть представлен в виде таблицы поиска с 2^n m-битовыми словами.

Как векторная булева функция S-блок задается своими так называемыми координатами или координатными функциями, т.е булевыми функциями $f_i: B^n \to B$,

$1 \le i \le m$, такие что $F = (f_1, f_2, .., f_m)$. Линейные комбинации m координатных функций S-блока $F : B^n \to B^m$ называют компонентами или компонентными функциями S-блока $F : B^n \to B^m$.

Одним из способов представления S-блока является таблица истинности. Таблица истинности S-блока представляет собой конкатенацию таблиц истинности всех его координатных функций.

Другим важным способом представления S-блока $F : B^n \to B^m$ является алгебраическая нормальная форма, т.е. представляющий его многочлен от n переменных над полем B^m вида

$$F(x_1, x_2, .., x_n) = a \oplus a_1 x_1 \oplus a_2 x_2 \oplus .. \oplus a_n x_n \oplus a_{12} x_1 x_2 \oplus a_{13} x_1 x_3 \oplus .. \oplus a_{12..n} x_1 x_2 ... x_n ,$$

где $a, a_1, a_2, .. a_n, a_{12}, a_{13}, .., a_{12..n} \in B^m$.

В случае представления S-блока $F : B^n \to B^m$ с помощью алгебраической нормальной формы важной характеристикой является алгебраическая степень $\deg(F)$, т.е. число переменных в самом длинном слагаемом её алгебраической нормальной формы.

Преобразование Фурье, преобразование Уолша, автокорреляционная функция для S-блока определяются с помощью соответствующих представлений компонентных функций S-блока.

Полезным способом представления S-блоков является также интерполяционный многочлен Лагранжа, на основе которого определяется такая важная характеристика как алгебраическая сложность S-блока.

Пример 1. (S-блоки блочного шифра DES (Data Encryption Standard [1])) DES использует 8 S-блоков $F: B^6 \to B^4$, осуществляющих замену 6-битных слов (a_1, a_2, a_3, a_4, a_5, a_6) на 4-битные (b_1, b_2, b_3, b_4) с помощью таблиц по следующему правилу. 4-битное слово (b_1, b_2, b_3, b_4) находится в соответствующей таблице на пересечении строки с номером (a_1, a_6) (два внешних бита входного 6-битного слова) и столбца с номером (a_2, a_3, a_4, a_5) (четыре внутренних бита входного 6-битного слова). Например, следующая таблица (рисунок 1) определяет первый из восьми S-блоков. С помощью нее входное слово «010101», которое имеет внешние биты «01» и внутренние биты «1010», заменяется на выходное слово «1111».

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	**1010**	1011	1100	1101	1110	1111
00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	**1111**	1010	0011	1001	1000	0110
10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

Рисунок 1 – Один из восьми S-блоков блочного шифра DES

Пример 2. (S-блок блочного шифра AES (Rijndael) (Advansed Encryption Standard [2]) AES использует 8-битный S-блок $F: B^8 \to B^8$, построенный с использованием ряда преобразований, предложенных в работе K. Nyberg [3], в комбинации с аффинным преобразованием. Также представляется следующей таблицей (рисунок 2) или перестановкой 256 элементов (десятичных или шестнадцатеричных чисел) (рисунок 3).

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

Рисунок 2 - S-блок блочного шифра AES.

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

Рисунок 3 - Перестановка, представляющая S-блок AES (шестнадцатеричная).

Пример 3. (S-блоки блочного шифра ГОСТ 28147-89 [4]) ГОСТ 28147-89 использует восемь 4-битных S-блоков $F: B^4 \to B^4$, не определяемые в самом стандарте. Конкретные значения определяются разработчиками алгоритмов, использующих стандарт. Например, криптопровайдер КриптоПро CSP [5] использует S-блоки, определяемые следующей таблицей (рисунок 4) [6].

S-блок	Значение															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
К1	9	6	3	2	8	B	1	7	A	4	E	F	C	0	D	5
К2	3	7	E	9	8	A	F	0	5	2	6	C	B	4	D	1
К3	E	4	6	2	B	3	D	8	C	F	5	A	0	7	1	9
К4	E	7	A	C	D	1	3	9	0	2	B	4	F	8	5	6
К5	B	5	1	9	8	D	F	0	E	4	2	3	C	7	A	6
К6	3	A	D	C	1	2	0	B	7	5	9	4	8	F	E	6
К7	1	D	2	9	7	A	6	0	8	C	4	5	F	3	B	E
К8	B	A	F	5	0	C	E	8	6	2	3	9	1	7	D	4

Рисунок 4 - S-блоки блочного шифра ГОСТ 28147-89 криптопровайдера КриптоПро CSP.

Пример 4. (S-блоки блочного шифра ГОСТ 34.12-2018 [7]) ГОСТ 34.12-2018 определяет два блочных шифра: блочный шифр «Кузнечик» («Kuznechik») с длиной блока n = 128 бит, блочный шифр «Магма» («Magma») с длиной блока n = 64 бит. Первый шифр использует 8-битный S-блок $F: B^8 \to B^8$, по утверждению авторов-разработчиков полученный с помощью случайного поиска с ограничением на параметры [8]. Однако в работах [9], [10] утверждение о случайности S-блока ставится под сомнение. В самом стандарте S-блок определяется как перестановка 256 чисел в десятичном виде (рисунок 5) или в шестнадцатеричном виде (рисунок 6):

252, 238, 221, 17, 207, 110, 49, 22, 251, 196, 250, 218, 35, 197, 4, 77, 233, 119, 240, 219, 147, 46, 153, 186, 23, 54, 241, 187, 20, 205, 95, 193, 249, 24, 101, 90, 226, 92, 239, 33, 129, 28, 60, 66, 139, 1, 142, 79, 5, 132, 2, 174, 227, 106, 143, 160, 6, 11, 237, 152, 127, 212, 211, 31, 235, 52, 44, 81, 234, 200, 72, 171, 242, 42, 104, 162, 253, 58, 206, 204, 181, 112, 14, 86, 8, 12, 118, 18, 191, 114, 19, 71, 156, 183, 93, 135, 21, 161, 150, 41, 16, 123, 154, 199, 243, 145, 120, 111, 157, 158, 178, 177, 50, 117, 25, 61, 255, 53, 138, 126, 109, 84, 198, 128, 195, 189, 13, 87, 223, 245, 36, 169, 62, 168, 67, 201, 215, 121, 214, 246, 124, 34, 185, 3, 224, 15, 236, 222, 122, 148, 176, 188, 220, 232, 40, 80, 78, 51, 10, 74, 167, 151, 96, 115, 30, 0, 98, 68, 26, 184, 56, 130, 100, 159, 38, 65, 173, 69, 70, 146, 39, 94, 85, 47, 140, 163, 165, 125, 105, 213, 149, 59, 7, 88, 179, 64, 134, 172, 29, 247, 48, 55, 107, 228, 136, 217, 231, 137, 225, 27, 131, 73, 76, 63, 248, 254, 141, 83, 170, 144, 202, 216, 133, 97, 32, 113, 103, 164, 45, 43, 9, 91, 203, 155, 37, 208, 190, 229, 108, 82, 89, 166, 116, 210, 230, 244, 180, 192, 209, 102, 175, 194, 57, 75, 99, 182.

Рисунок 5 - Перестановка, представляющая S-блок шифра «Кузнечик» (десятичная).

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

Рисунок 6 - Перестановка, представляющая S-блок шифра «Кузнечик» (шестнадцатеричная).

Второй шифр стандарта является вариантом алгоритма ГОСТ 28147-89 с фиксированными восемью 4-битными S-блоками $F: B^4 \to B^4$.

1 National Institute of Standards and Technology (1979). “FIPS-46: Data Encryption Standard (DES).” Revised as FIPS 46-1:1988, FIPS 46-2:1993, FIPS 46-3:1999, http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

2 NIST, FIPS PUB 197, "Advanced Encryption Standard (AES)," November 2001., http://csrc.nist.gov/publications/fips/fips197/ fips-197.{ps,pdf}

3 Nyberg, K. (1994). Differentially uniform mappings for cryptography. In: Helleseth, T. (eds) Advances in Cryptology — EUROCRYPT ’93. EUROCRYPT 1993. Lecture Notes in Computer Science, vol 765. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48285-7_6

4 ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»

5 https://www.cryptopro.ru/products/csp

6 V. Popov, I. Kurepkin, S. Leontiev, Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms, RFC 4357, January 2006

7 ГОСТ 34.12-2018 «Информационная технология (ИТ). Криптографическая защита информации. Блочные шифры»

8 Vasily Shishkin, Grigory Marshalko, A Memo on Kuznyechik S-Box, ISO/IEC JTC 1/SC 27/WG 2 - Cryptography and security mechanisms, N 1804, 2018-09-27

9 Alex Biryukov, Léo Perrin, and Aleksei Udovenko. Reverse-engineering the S-box of streebog, kuznyechik and STRIBOBr1. Cryptology ePrint Archive, Report 2016/071, 2016. http://eprint.iacr.org/2016/071.

10 Léo Perrin. Partitions in the S-box of Streebog and Kuznyechik. IACR Trans. Symmetric Cryptol., 2019(1):302–329, 2019.