УДК 004.9
https://doi.org/10.47533/2020.1606-146X.176

Е. Н. СЕЙТКУЛОВ[1]*, Р. М. ОСПАНОВ[1], Б. Б.ЕРГАЛИЕВА[1], А. Т. АХМЕДИЯРОВА[2]

[1]Евразийский национальный университет им. Л.Н.Гумилева,
Нур-Султан, Казахстан
e-mail: yerzhan.seitkulov@gmail.com
[2]Центр научных и научно-технических исследований National Security
Алматы, Казахстан

АЛГЕБРАИЧЕСКИЕ МЕТОДЫ ГЕНЕРАЦИИ ОПТИМАЛЬНЫХ S-БЛОКОВ

В работе выполнен обзор алгебраических методов генерации криптографических S-блоков. В данной работе рассмотрены методы генерации S-блоков, основанные на применении полиномиальных преобразований (линейных, квадратичных, кубических), дробно-линейных преобразований и других специальных видов алгебраических преобразований. Также приведен ряд примеров генерации S-блоков с помощью квазигрупп и других алгебраических структур. Рассмотренные методы генерации S-блоков позволяют получить новые S-блоки, обладающие необходимыми криптографическими свойствами, такими же или даже лучше, чем у S-блока, построенного для алгоритма Rijndael.

Ключевые слова*: информационная безопасность, криптография, криптографические алгоритмы, S-блоки, алгебраические методы.*

Введение. Одной из важных и сложных задач в современной криптографии является нахождение эффективных методов генерации криптографических оптимальных S-блоков, определяющих устойчивость криптографических алгоритмов к различным криптоаналитическим атакам. В данной работе рассматривается алгебраический подход к решению этой задачи. При алгебраических методах S-блоки проектируются в соответствии с некоторыми доказанными математическими соотношениями и принципами. Классическим алгебраическим методом генерации S-блоков является метод, с помощью которого был построен S-блок для алгоритма Rijndael [1] (победитель конкурса AES). Существует ряд модификаций такого метода, основанные на варьировании выбора определенного неприводимого многочлена, по модулю которого определяется умножение в поле $GF(2^8)$, выбора первого преобразования из альтернативных преобразований в работе Ниберга [2], выбора определенной матрицы аффинного преобразования и выбора определенной сдвиговой константы. В работе [3] представлен обзор методов генерации Rijndael S-блоков и их модификаций, а также обобщенный алгебраический метод конструирования 8-битных Rijndael S-блоков. В данной работе дается обзор других алгебраических методов генерации S-блоков, существенно отличающихся от вышеуказанных. Рассматриваются методы генерации S-блоков, основанные на применении полиномиальных преобразований (линейных, квадратичных, кубических), дробно-линейных преобразований и других специальных видов алгебраических преобразований. Также приводится ряд приме-

* E-mail корреспондирующего автора:yerzhan.seitkulov@gmail.com

ров генерации S-блоков с помощью квазигрупп и других алгебраических структур, эллиптических кривых, теории графов. Рассматриваемые методы генерации S-блоков позволяют получить новые S-блоки, обладающие необходимыми криптографическими свойствами, такими же или даже лучше, чем у S-блока, построенного для алгоритма Rijndael.

Алгебраические методы. Как известно, для симметричного блочного алгоритма шифрования Rijndael S-блок конструируется на основе выбора определенного неприводимого многочлена, по модулю которого определяется умножение в поле $GF(2^8)$, выбора первого преобразования из альтернативных преобразований из работы Ниберга, выбора определенной матрицы аффинного преобразования и выбора определенной сдвиговой константы. Аналогичным образом можно построить другие S-блоки, варьируя наборы выбираемых компонентов, используемых в конструкции наподобие Rijndael S-блока. Таким образом, был создан ряд модификаций построения Rijndael-подобных S-блоков. А в работе [3] был представлен обобщенный алгебраический метод конструирования 8-битных Rijndael S-блоков. Однако существует ряд других алгебраических методов генерации S-блоков, существенно отличающихся от методов построения Rijndael S-блоков и их модификаций.

Существуют методы генерации S-блоков, основанные на применении полиномиальных преобразований (линейных, квадратичных, кубических).

Например, в работе [4] предлагается алгебраический метод получения динамических S-блоков с использованием линейного полиномиального преобразования и перестановки. Метод состоит из следующих основных этапов.

1. Применяется преобразование $F : GF(2^n) \to GF(2^n)$, определяемое формулой $F(x) = (ax + b)\ mod\ (2^n + 1)$, где $a, b, x \in GF(2^n)$, $a \neq 0$.

2. К результату первого этапа применяется модулярная мультипликативная инверсия по модулю $mod\ (2^n + 1)$.

3. Далее к полученному результату применяется перестановка.

В работе [5] предлагается еще один алгебраический метод получения динамических S-блоков с использованием полиномиального квадратичного преобразования, динамического аффинного преобразования и перестановочной техники создания окончательного S-блока. Метод состоит из следующих основных этапов.

1. Применяется квадратичное преобразование $F : GF(2^n) \to GF(2^n)$, определяемое формулой $F(x) = (a^2x + b)\ mod 2^n$, где $a, b, x \in GF(2^n)$, $a \neq 0$.

2. К результату первого этапа применяется модулярная мультипликативная инверсия по модулю $mod\ (2^n + 1)$.

3. Далее применяется динамическое аффинное преобразование.

4. Далее к полученному результату применяется динамическая перестановка.

В работе [6] S-блок $F : GF(2^n) \to GF(2^n)$ определяется формулой кубического преобразования $F(x) = (a^3x + b)\ mod\ (2^n + 1)$, где $a, b, x \in GF(2^n)$, $a \neq 0$. Так, например, 8-битный S-блок $F : GF(2^8) \to GF(2^8)$ определяется как $F(x) = \begin{cases} (63x^3 + 100)(\mathrm{mod}\,257), & x \neq 135 \\ 31, & x = 135 \end{cases}$.

При $x = 135$ $F(x) \notin GF(2^8)$, поэтому для сохранения биективности для этих значений x значение $F(x)$ доопределяется как 31 при $x = 135$.

Существуют методы генерации S-блоков, основанные на применении дробно-линейных преобразований и других специальных видах алгебраических преобразований.

Например, в работе [7] S-блок $F : GF(2^8) \to GF(2^8)$ определяется как композиция $F = g \circ f$ двух преобразований. Первое преобразование определяется как $g(x) = \dfrac{ax+b}{cx+d}$, где $a, b, c, d \in GF(2^8)$ и $ad - bc \neq 0$. Это преобразование является дробно-линейным преобразованием (известное как преобразование Мёбиуса), определяющее действие проективной общей линейной группы $PGL(2, GF(2^8))$ на $GF(2^8)$. С помощью этого действия можно построить 16776960 S-блоков. S-блок строится путем вычисления $g(x)$ для фиксированных значений a, b, c, $d \in GF(2^8)$ для каждого элемента $x \in GF(2^8)$ с проверкой условий $ad - bc \neq 0$ и $cx + d \neq 0$. Числа, полученные в результате вычисления $g(x)$ затем преобразуются в двоичную форму и представляются как степень w, где w – корень примитивного неприводимого многочлена. Неприводимый многочлен, по модулю которого определяется умножение в поле $GF(2^8)$, выбирается из списка 30 неприводимых многочленов степени 8 [8]. Второе преобразование f является перестановкой определенного типа из симметрической группы S_{256}, Это преобразование позволяет изменить положение элементов, а также разрушить структуру поля Галуа. В табличной форме эта перестановка следующая:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	212	16	44	114	149	42	176	240	76	160	96	189	207	251	84	214
1	112	229	228	230	196	8	201	191	159	106	125	110	164	117	33	249
2	213	155	248	167	56	116	69	38	177	206	192	58	70	172	87	204
3	217	168	123	145	238	77	127	173	63	99	80	62	246	133	137	85
4	244	129	78	83	161	9	209	183	25	59	12	188	90	73	171	113
5	35	236	130	163	158	242	187	134	57	18	100	225	92	142	13	150
6	200	24	170	5	237	36	148	147	140	72	71	154	165	174	184	21
7	239	75	97	151	152	128	256	215	231	51	136	105	232	61	226	107
8	26	88	182	68	198	143	4	233	54	43	46	120	22	220	52	60
9	19	181	29	11	30	245	175	89	104	178	79	45	2	103	241	193
10	47	202	6	223	221	243	3	40	115	95	14	93	64	32	144	81
11	190	162	141	180	101	119	124	28	254	210	7	253	109	224	37	186
12	250	74	1	194	205	131	10	219	146	135	23	132	98	126	66	203
13	41	121	195	252	185	255	208	122	222	227	53	20	86	234	102	211
14	49	39	138	48	65	139	199	91	179	67	235	15	216	157	247	34
15	50	108	153	169	197	156	111	27	118	82	218	31	17	55	166	94

Таким образом, $F(a) = f(g(a))$ для любого $a \in GF(2^8)$.

Так, например, в работе [9] S-блок $F : GF(2^8) \to GF(2^8)$ строится с помощью дробно-линейного преобразования $g(x) = \dfrac{ax+b}{cx+d}$, где $a = 35 \in GF(2^8)$ $b = 15 \in GF(2^8)$ $c = 9 \in GF(2^8)$ $d = 5 \in GF(2^8)$ и перестановки, задаваемой следующей таблицей.

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

Аналогично в работе [10] S-блок $F : GF(2^8) \to GF(2^8)$ строится с помощью дробно-линейного преобразования $F(x) = \begin{cases} \dfrac{ax+b}{cx+d}, x \neq 47 \\ 149, x = 47 \end{cases}$, где $a = 29 \in GF(2^8)$ $b = 15 \in GF(2^8)$ $c = 8 \in GF(2^8)$ $d = 5 \in GF(2^8)$. При $x = 47$ знаменатель обращается в 0, поэтому для сохранения биективности для этго значения x значение $F(x)$ доопределяется как 149. Неприводимый многочлен, по модулю которого определяется умножение в поле $GF(2^8)$, $m(x) = x^8 + x^6 + x^5 + x^4 + 1$.

В другой работе [11] S-блок $F : GF(2^8) \to GF(2^8)$ строится с помощью дробно-линейного преобразования $F(x) = \dfrac{ax+b}{cx+d}$, где $a = 45 \in GF(2^8)$ $b = 10 \in GF(2^8)$ $c = 2 \in GF(2^8)$ $d = 9 \in GF(2^8)$.

В работе [12] S-блок $F : GF(2^n) \to GF(2^n)$ строится с помощью так называемого дробно-кубического преобразования $F(x) = \dfrac{1}{cx^3 + \beta} \bmod(2^n + 1)$, где $\alpha, \beta, x \in GF(2^n)$, α, β не равно 0 одновременно, $\alpha x3 + b \neq 0$. Так, например, 8-битный S-блок $F : GF(2^8) \to GF(2^8)$ определяется как $F(x) = \begin{cases} \dfrac{1}{95x^3 + 15} \bmod(2^8 + 1), x \neq 176, x \neq 184 \\ 0, x = 176 \\ 106, x = 184 \end{cases}$. При $x = 176$ $\dfrac{1}{95x^3 + 15} \bmod(2^8 + 1) \notin GF(2^8)$, а при $x = 184$ $95\,x^3 + 15 = 0$, поэтому для сохранения

биективности для этих значений x значение $F(x)$ доопределяется как 0 при $x = 176$ и 106 при $x = 184$.

В [13] S-блок $F : GF(2^8) \to GF(2^8)$ определяется по формуле:

$$F(x)\begin{cases} \dfrac{A \times x \otimes \alpha}{A \times x \otimes \beta}, \text{ если } x \neq A^{-1} \times \beta \\ 01 \text{ (в шестнадцатеричном представлении), если } x = A^{-1} \times \beta \end{cases},$$

где $A = \begin{pmatrix} 10001101 \\ 11000110 \\ 01100011 \\ 10110001 \\ 11011000 \\ 01101100 \\ 00110110 \\ 00011011 \end{pmatrix}$, $\alpha = FE$, $\beta = 3F$ (в шестнадцатеричном представлении).

Умножение в поле $GF(2^8)$ выполняется по модулю неприводимого многочлена $m(x) = x^8 + x^4 + x^3 + x^1$.

Существуют методы генерации S-блоков, основанные на применении квазигрупп и других алгебраических структур.

Например, в работе [14] предлагается метод построения криптографически стойких 4-битовых S-блоков с использованием квазигрупп порядка 4. Цель работы – предоставить итеративный инструмент для проектирования криптографически стойких S-блоков (в [14] обозначаемых как Q-S-блоки, поскольку их построение осуществляется квазигруппами) для будущих разработок в симметричной низкоресурсной (легковесной) криптографии. Этот метод позволяет работать в основном с несколькими разными стойкими S-блоками, повторно используя только одну аппаратную схему и просто изменяя несколько параметров. Метод состоит из следующих основных шагов. Соответствующие определения можно найти в [14].

Шаг 1. Выбирается одна нелинейная квазигруппа порядка 4.

Шаг 2. Задается количество раундов.

Шаг 3. Задаются лидеры. Обычно их количество совпадает с количеством раундов.

Шаг 4. Генерируются все возможные входные 4-битовые блоки в лексикографическом порядке (их общее количество $2^4 = 16$).

Шаг 5. Для каждого входного блока выполняются следующие шаги:

Шаг 5.1. К входному блоку применяется e-преобразование с лидером ℓ.

Шаг 5.2. Изменяется полученный выше результат и снова применяется e-преобразование с уже другим лидером ℓ.

Шаг 5.3. Эти шаги повторяются столько раз, сколько есть количество раундов.

Шаг 5.4. Сохраняется 4-битный результат последнего раунда.

Шаг 6. В конце объединяются все сохраненные результаты, генерируя перестановку порядка 16 или 4-битный Q-S-блок.

Далее выполняется проверка оптимальности полученного S-блока.

В работе [15] предлагается метод построения 8-битовых S-блоков, основанный на применении действия проективной специальной линейной группы $PSL(2,\mathbb{Z})$ на проективной линии $PL(GF(7))$ над конечным полем $GF(7)$. Метод состоит из следующих основных шагов.

Шаг 1. Выполняется действие проективной специальной линейной группы $PSL(2,\mathbb{Z}) = \langle x, y : x^2 = y^2 = 1 \rangle$ на проективной линии $PL(GF(7)) = GF(7) \cup \infty = \{0,1,2,3,4,5,6,\infty\}$ над конечным полем $GF(7)$. В результате получается группа перестановок G, порождаемая $\overline{x} = (0\,\infty)(1\,6)(2\,3)(4\,5)$ и $\overline{y} = (0\,\infty\,1)(2\,4\,6)(3)(5)$.

Шаг 2. Рисуется диаграмма смежных классов, используя перестановки $\overline{x}$ и $\overline{y}$. Диаграмма смежных классов – это графический способ представления перестановочного действия конечно порожденной группы. На рисунке 1 показана диаграмма смежных классов, полученная для группы перестановок G. Поскольку $\overline{x}$ и $\overline{y}$ имеют порядок 2 и 3 соответственно, порождающий $\overline{x}$ обозначается ребром, а порождающий $\overline{y}$ изображается треугольником. Вершины треугольника переставлены против часовой стрелки, а фиксированные точки $\overline{y}$ обозначены жирными точками на диаграмме смежных классов.

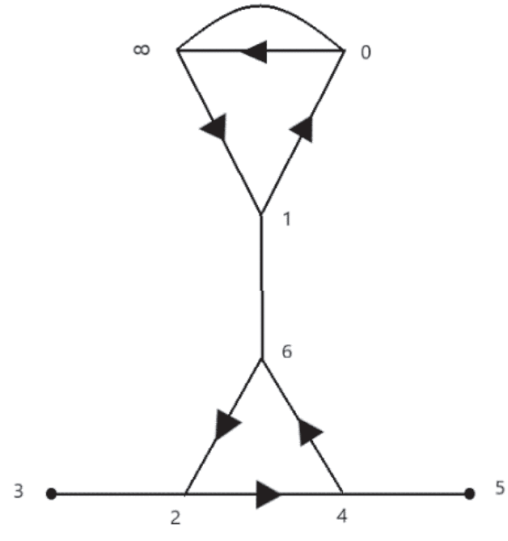

Рисунок 1 – Диаграмма смежных классов для группы перестановок G.

Шаг 3. Строится матрица смежности M из диаграммы смежных классов для действия $PSL(2,\mathbb{Z})$ на $PL(GF(7))$. Матрица смежности ориентированного графа $G = (V, E)$, где V — множество вершин, а E — множество ребер, имеет значение 1 на своей (i, j)-й позиции, если существует ребро из v_i в v_j, где $v_1, v_2, ..., v_n$ – произвольный список вершин ориентированного графа. Т.е. элементы $M = (m_{ij})$ матрицы смежности ориентированного графа определяются следующим образом:

$$m_{ij} = \begin{cases} 1, & \text{если } (v_i, v_j) \text{ – ребро G} \\ 0 & \text{в противном случае} \end{cases}.$$

В диаграмме смежных классов на рисунке 1 вершины помечены как 0, 1, 2, 3, 4, 5, 6 и ∞. Из рисунка видно, что существует ребро от 0 до 1, поэтому в матрица смежности элемент, расположенный на пересечении 1-й строки и 8-го столбца, равен 1, а все остальные элементы 1-й строки равны 0. Точно так же во 2-й строке матрицы смежности 1-й и 7-й элементы равны 1, потому что существует ребро от 1 до 0 и от 1 до 6. Все остальные элементы в этой строке равны нулю. Таким же образом, заполняя оставшиеся элементы в матрице, в результате формируется следующая матрица смежности M:

$$M = \begin{pmatrix} 00000001 \\ 10000010 \\ 00011000 \\ 00110000 \\ 00000110 \\ 00001100 \\ 01100000 \\ 11000000 \end{pmatrix}.$$

Шаг 4. К элементам поля $GF(2^8)$ применяются преобразования T_k, определяемые следующим образом: $T_k(t_n) = Mt_n + \sum_{r \in I_k} t_{n+r(\mathrm{mod}\,256)}$, где $t_n \in GF(2^8)$ в 8-битной двоичной форме, $n = 0, 1, 2, ..., 255$, $k = 1, 2, ..., 8$, I_k – 8 различных множеств целых чисел $I_1 = \{1, 2, 3, ..., 128\}$, $I_2 = \{2, 4, 6, ..., 128\}$, $I_3 = \{4, 8, 12, ..., 128\}$, $I_4 = \{8, 16, 24, ..., 128\}$, $I_5 = \{16, 32, 48, ..., 128\}$, $I_6 = \{32, 64, 96, ..., 128\}$, $I_7 = \{64, 128\}$, $I_8 = \{128\}$ а M – матрица, построенная на предыдущем шаге. Например, для $k = 7$ $T_7(t_n) = Mt_n + t_{n+64(\mathrm{mod}\,256)} + t_{n+128(\mathrm{mod}\,256)}$. Аналогично, для $k = 8$ $T_8(t_n) = Mt_n + t_{n+128(\mathrm{mod}\,256)}$. В результате применения преобразований $T_1, \ldots, T_8$ получаются 8 различных 8-битовых S-блоков.

Существует множество еще других алгебраических методов генерации подстановок, например, [16], [17]. Их все объединяет то, что они были получены в результате многочисленных исследований, направленных на поиск наиболее эффективных методов построения оптимальных S-блоков. Рассмотренные методы генерации S-блоков позволяют получить новые S-блоки, обладающие необходимыми криптографическими свойствами, такими же или даже лучше, чем у S-блока, построенного для алгоритма Rijndael.

Заключение. В данной работе рассмотрен ряд алгебраических методов генерации криптографических S-блоков. Классическим алгебраическим методом генерации S-блоков является метод конструирования Rijndael S-блоков. Существующие модификации этого метода основаны на варьировании выбора определенного неприводимого многочлена, по модулю которого определяется умножение в поле $GF(2^8)$, выбора первого преобразования из альтернативных преобразований в работе Ниберга, выбора определенной матрицы аффинного преобразования и выбора определенной

сдвиговой константы. В результате многочисленных исследований, направленных на поиск наиболее эффективных методов построения оптимальных S-блоков, был построен ряд других алгебраических методов генерации S-блоков, существенно отличающихся от метода конструирования Rijndael S-блоков. В данной работе рассмотрены методы генерации S-блоков, основанные на применении полиномиальных преобразований (линейных, квадратичных, кубических), дробно-линейных преобразований и других специальных видов алгебраических преобразований. Также приведен ряд примеров генерации S-блоков с помощью квазигрупп и других алгебраических структур. Рассмотренные методы генерации S-блоков позволяют получить новые S-блоки, обладающие необходимыми криптографическими свойствами, такими же или даже лучше, чем у S-блока, построенного для алгоритма Rijndael.

Благодарности. Работа выполнена при финансовой поддержке КН МОН РК, № AP09258274

ЛИТЕРАТУРА

1 Daemen, J., Rijmen, V. The Design of Rijndael: AES - The Advanced Encryption Standard // Springer-Verlag Berlin Heidelberg, 2002, 238 p., doi: 10.1007/978-3-662-04722-4.

2 Nyberg, K. Differentially uniform mappings for cryptography // Advances in Cryptology, Proc. Eurocrypt'93, LNCS 165, T. Helleseth, Ed., Springer-Verlag, 1994, pp. 55-64.

3 Оспанов Р., Сейткулов Е., Ергалиева Б. обобщенный алгебраический метод конструирования 8-битных rijndael S-блоков // Вестник КазАТК, 120(1), 156–163. https://doi.org/10.52167/1609-1817-2022-120-1-156-163

4 A. H. Zahid, E. Al-Solami and M. Ahmad, "A Novel Modular Approach Based Substitution-Box Design for Image Encryption," in IEEE Access, vol. 8, pp. 150326-150340, 2020, doi: 10.1109/ACCESS.2020.3016401.

5 Zahid A. H. et al. Dynamic S-Box Design Using a Novel Square Polynomial Transformation and Permutation // IEEE Access, vol. 9, pp. 82390-82401, 2021, doi: 10.1109/ACCESS.2021.3086717.

6 Zahid A.H., Arshad M.J. An Innovative Design of Substitution-Boxes Using Cubic Polynomial Mapping. Symmetry 2019, 11, 437.

7 Altaleb A., Saeed M.S., Hussain I., Aslam M. An algorithm for the construction of substitution box for block ciphers based on projective general linear group. AIP Advances. 2017, 7, 035116

8 Church, R. Tables of irreducible polynomials for the first four prime moduli // The Annals of Maths., 2nd Series, vol. 36, no. 1, pp. 198-209, Jan (1935) http://www .jstor.org/stable/1968675.

9 Nizam Chew L.C., Ismail E.S. S-box Construction Based on Linear Fractional Transformation and Permutation Function. Symmetry 2020, 12, 826.

10 Farwa, Shabieh & Idrees, Lubna. (2016). A highly nonlinear S-box based on a fractional linear transformation. SpringerPlus. 5. 10.1186/s40064-016-3298-7.

11 Iqtadar Hussain,Tariq Shah, Muhammad Asif Gondal, Majid Khan and Waqar Ahmad Khan Construction of New S-box using a Linear Fractional Transformation // World Applied Sciences Journal 14 (12): 1779-1785, 2011

12 Zahid, A.H., Arshad, M.J., Ahmad, M.: A novel construction of efficient substitution-boxes using cubic fractional transformation, Entropy 21 (2019), no. 3, Paper No. 245 (2019)

13 Nitaj A., Susilo W., Tonien J. A New Improved AES S-box with Enhanced Properties // Liu J., Cui H. (eds) Information Security and Privacy. ACISP 2020. Lecture Notes in Computer Science, vol 12248. Springer, Cham. 2020. https://doi.org/10.1007/978-3-030-55304-3_7

14 Mihajloska, H., Gligoroski, D. Construction of Optimal 4-bit S-boxes by Quasigroups of Order 4 // SECURWARE 2012 : The Sixth International Conference on Emerging Security Information, Systems and Technologies, 2012, pp. 163-168.

15 Siddiqui N, Yousaf F, Murtaza F, Ehatisham-ul-Haq M, Ashraf MU, Alghamdi AM, et al. (2020) A highly nonlinear substitution-box (S-box) design using action of modular group on a projective line over a finite field. PLoS ONE 15(11): e0241890. https://doi.org/10.1371/journal.pone.0241890

16 Hussain S., Jamal S. S., Shah T., Hussain I. A Power Associative Loop Structure for the Construction of Non-Linear Components of Block Cipher. IEEE Access, vol. 8, pp. 123492-123506, 2020

17 Gao W., Idrees B., Zafar S., Rashid T. Construction of Nonlinear Component of Block Cipher by Action of Modular Group PSL(2, Z) on Projective Line PL(GF(28)). IEEE Access, vol. 8, pp. 136736-136749, 2020

Е. Н. СЕЙТҚҰЛОВ[1], Р. М. ОСПАНОВ[1], Б. Б. ЕРҒАЛИЕВА[1], А. Т. АХМЕДИЯРОВА[2]

[1]Л.Н.Гумилев атындағы Еуразия ұлттық университеті
Нұр-Сұлтан, Қазақстан
e-mail: yerzhan.seitkulov@gmail.com
[2]National Security ғылыми және ғылыми-техникалық зерттеулер орталығы
Алматы, Қазақстан

ОПТИМАЛДЫ S-БЛОКТАРДЫ ТУЫНДАУДЫҢ АЛГЕБРАЛЫҚ ӘДІСТЕРІ

Жұмыста криптографиялық S-блоктарды құрудың алгебралық әдістеріне шолу ұсынылған. Бұл жұмыста біз көпмүшелік түрлендірулерді (сызықтық, квадраттық, кубтық), бөлшек сызықтық түрлендірулерді және алгебралық түрлендірулердің басқа да арнайы түрлерін пайдалану негізінде S-блоктарды генерациялау әдістерін қарастырамыз. Сондай-ақ, квазигруппаларды және басқа алгебралық құрылымдарды пайдаланып S-блоктарын құрудың бірқатар мысалдары келтірілген. S-блоктарын генерациялаудың қарастырылған әдістері Rijndael алгоритмі үшін құрастырылған S-блоктарымен бірдей немесе тіпті жақсырақ қажетті криптографиялық қасиеттері бар жаңа S-блоктарын алуға мүмкіндік береді.

Түйін сөздер*: ақпараттық қауіпсіздік, криптография, криптографиялық алгоритмдер, S-блоктары, алгебралық әдістер.*

YERZHAN N. SEITKULOV[1], RUSLAN M. OSPANOV[1], BANU B. YERGALIYEVA[1], AINUR AKHMEDIYAROVA[2]

[1]Gumilyov Eurasian National University
Nur-Sultan, Kazakhstan
e-mail: yerzhan.seitkulov@gmail.com
[2]Center for Scientific and Scientific and Technical Research National Security
Almaty, Kazakhstan

ALGEBRAIC METHODS FOR GENERATING OPTIMAL S-BLOCKS

The paper presents a review of algebraic methods for generating cryptographic S-boxes. In this paper, we consider methods for generating S-boxes based on the use of polynomial transformations (linear, quadratic, cubic), fractional linear transformations, and other special types of algebraic transformations. A number of examples of generating S-boxes using quasigroups and other algebraic structures are also given. The considered methods for generating S-boxes make it possible to obtain new S-boxes that have the necessary cryptographic properties that are the same or even better than those of the S-box built for the Rijndael algorithm.

***Key words**: information security, cryptography, cryptographic algorithms, S-boxes, algebraic methods.*