

Группы автоморфизмов максимально рассеивающих матриц

Буров Д.А., Костарев С.В.

Классическим примером построения алгоритмов блочного шифрования являются XSL–алгоритмы, раундовое преобразование которых состоит из прибавления ключа (X–слой), параллельного действия s–боксов (S–слой) и линейного рассеивающего преобразования (L–слой).

Алгоритмы блочного шифрования, являющиеся XSL–алгоритмами

- Кузнечик (ГОСТ Р 34.12-2015)
- AES
- Khazad
- Anubis

Коэффициенты рассеивания матрицы

Определение

Коэффициентом рассеивания квадратной матрицы A порядка n над полем $\mathbb{F}_{2^r}$ называется величина

$$\beta(A) = \min_{x \in \mathbb{F}_{2^r}^n, x \neq 0} (w(x) + w(xA)).$$

Определение

Квадратная матрица A порядка n над полем $\mathbb{F}_{2^r}$ называется максимально рассеивающей (MP-) матрицей, если $\beta(A) = n + 1$.

Некоторые способы построения МР–матриц

Случайный выбор из «специального» класса матриц

- циркулянтные матрицы ^a
- FFH–матрицы ^b

^aAES, Whirlpool

^bKhazad, Anubis, Clefia

Алгебраические методы

- конструкции на основе матриц Вандермонда
- конструкции на основе матриц Коши ^a
- использование рекурсивных МДР кодов ^b

^aСтрибог (ГОСТ 34.11 2018)

^bКузнечик, Photon, LED

Группа автоморфизмов матрицы

Определим действие группы $G < S_n \times S_n$ на $(\mathbb{F}_{2^r})_{n,n}$ следующим образом. Если $A = (a_{i,j}) \in (\mathbb{F}_{2^r})_{n,n}$ и $g = (g_1, g_2) \in G$, то

$$A^g = A^{(g_1, g_2)} = \widehat{g}_1^{-1} A \widehat{g}_2 = (a_{g_1(i), g_2(j)}),$$

где $\widehat{g}_1, \widehat{g}_2$ — подстановочные матрицы, соответствующие подстановкам $g_1, g_2 \in S_n$.

Определение

Группой автоморфизмов матрицы $A \in (\mathbb{F}_{2^r})_{n,n}$ будем называть

$$\text{Aut}(A) = \{g \in S_n \times S_n \mid A^g = A\}.$$

Данное понятие возникает, например, в связи с изучением группы автоморфизмов графа¹.

¹Chao C. «On groups and graphs», 1965

Определение

Квадратная матрица A порядка n над полем $\mathbb{F}_{2^r}$ вида

$$A = \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_0 \end{pmatrix}$$

называется циркулянтном.

Через $\mathbb{Z}_n^+$ будем обозначать правое регулярное представление группы $(\mathbb{Z}_n, +)$.

Утверждение

Пусть $A = (a_{i,j})$ квадратная матрица порядка n над полем $\mathbb{F}_{2^r}$ и $\text{Aut}(A) = \{(g, g) \mid g \in G\}$, $G < S_n$. Тогда A является циркулянтном в том и только том случае, когда $\mathbb{Z}_n^+ < G$.

Определение

Квадратная матрица A порядка 2^n над полем $\mathbb{F}_{2^r}$ называется FFH-матрицей, если

$$A = \begin{pmatrix} U & V \\ V & U \end{pmatrix},$$

где U, V — FFH-матрицы размера $2^{n-1} \times 2^{n-1}$.

Через $(\mathbb{Z}_2^n)^+$ будем обозначать правое регулярное представление группы $(\mathbb{Z}_2^n, +)$.

Утверждение

Пусть $A = (a_{i,j})$ — квадратная матрица порядка 2^n над полем $\mathbb{F}_{2^r}$ и $\text{Aut}(A) = \{(g, g) \mid g \in G\}$, $G < S_{2^n}$. Тогда A является FFH-матрицей в том и только том случае, когда $(\mathbb{Z}_2^n)^+ < G$.

Утверждение (MacWilliams F., Sloane N., 1977)

Матрица $A \in (\mathbb{F}_{2^r})_{n,n}$ является МР-матрицей тогда и только тогда, когда все ее квадратные подматрицы невырождены.

FFH-матрица порядка 4

A	B	C	D
B	A	D	C
C	D	A	B
D	C	B	A

Циркулянт порядка 4

A	B	C	D
D	A	B	C
C	D	A	B
B	C	D	A

Таблица: Число различных миноров в матрице порядка 8 с группой автоморфизмов $\text{Aut}(A) = \{(g, g) \mid g \in G\}$, $G < S_8$, и число МР-матриц в выборке объема 10^6 над полем $\mathbb{F}_{2^8}$.

G	Порядок подматрицы	Общее число миноров	Число МР-матриц в выборке объема 10^6
	$\mathbb{Z}_8^+$	937	20008
	$(\mathbb{Z}_4 \times \mathbb{Z}_2)^+$	946	22406
	$(\mathbb{Z}_2^3)^+$	962	152730
	$\mathbb{Z}_7^+$	1597	12655
	Q_8	1597	1280
	D_4^+	1621	1535
	$\mathbb{Z}_4^+$	3221	0
	$\mathbb{Z}_2^+$	4469	0

Подход к синтезу, предлагаемый в работе

Предлагается «искать» преобразования с оптимальными или близкими к оптимальным параметрами в классах преобразований с нетривиальной группой автоморфизмов.

Ранее этот подход был использован для построения подстановок поля $\mathbb{F}_{2^n}$ с высокими криптографическими характеристиками.²³

²Burov D., Kostarev S., Menyachikhin A., «Class of piecewise-monomial mappings: differentially 4-uniform permutations of $\mathbb{F}_{2^n}$ with graph algebraic immunity 3 exist», CTCrypt 2023.

³Буров Д., Костарев С. «Некоторые криптографические свойства кусочно-мономиальных преобразований поля $\mathbb{F}_{2^n}$ », CTCrypt 2024. 

Лишние симметрии могут «испортить» линейное преобразование

Если дополнительно симметризовать циркулянт с помощью инволюции $h = (h_1, h_2) \in S_4 \times S_4$, где

$$h_1 = h_2 = (1)(3)(2, 4) \in S_4,$$

то получим следующую матрицу

<table border="1"><tr><td>A</td><td>B</td><td>C</td><td>D</td></tr><tr><td>D</td><td>A</td><td>B</td><td>C</td></tr><tr><td>C</td><td>D</td><td>A</td><td>B</td></tr><tr><td>B</td><td>C</td><td>D</td><td>A</td></tr></table>	A	B	C	D	D	A	B	C	C	D	A	B	B	C	D	A	$\Rightarrow$	<table border="1"><tr><td>A</td><td>B</td><td>C</td><td>B</td></tr><tr><td>B</td><td>A</td><td>B</td><td>C</td></tr><tr><td>C</td><td>B</td><td>A</td><td>B</td></tr><tr><td>B</td><td>C</td><td>B</td><td>A</td></tr></table>	A	B	C	B	B	A	B	C	C	B	A	B	B	C	B	A
A	B	C	D																															
D	A	B	C																															
C	D	A	B																															
B	C	D	A																															
A	B	C	B																															
B	A	B	C																															
C	B	A	B																															
B	C	B	A																															
$\langle g \rangle \cong \mathbb{Z}_4^+$		$\langle g, h \rangle \cong D_4$																																

Далее для подгруппы $P < S_n \times S_n$ через $P_1, P_2 < S_n$ обозначим проекции P на первую и вторую координаты соответственно.

Утверждение

Пусть $A \in GL(n, 2^r)$. Тогда $\text{Aut}(A)_1 \cong \text{Aut}(A)_2$ и

$$\text{Aut}(A) = \{(g_1, \sigma(g_1)) \mid g_1 \in \text{Aut}(A)_1\},$$

где $\sigma: \text{Aut}(A)_1 \rightarrow \text{Aut}(A)_2$ — изоморфизм групп. В частности, если A является МР-матрицей, то $\sigma: g \mapsto t^{-1}gt$, $g \in \text{Aut}(A)_1$.

Из утверждения следует, что группа автоморфизмов матрицы однозначно определяется парой (G, σ) , где $G < S_n$, а σ — изоморфизм подгрупп в S_n .

$$\text{Aut}(A) = \{(g, \sigma(g)) \mid g \in G\} =: (G, \sigma).$$

Через $M_{n,r}(G, \sigma)$, $G < S_n$, обозначим подмножество матриц в $GL(n, 2^r)$ с группой автоморфизмов (G, σ) , т.е.

$$M_{n,r}(G, \sigma) = \{A \in GL(n, 2^r) \mid \text{Aut}(A) = \{(g, \sigma(g)) \mid g \in G\}\}.$$

Утверждение

Пусть $G < S_n$ и для некоторого $t \in S_n$ выполнено равенство $\sigma: g \mapsto t^{-1}gt, g \in G$. Тогда

$$M_{n,r}(G, \sigma) = M_{n,r}(G, 1)\hat{t}.$$

При изучении свойств МР-матриц достаточно рассматривать случай

$$\text{Aut}(A) = \{(g, g) \mid g \in G\} = (G, 1).$$

Определение

Транзитивная нерегулярная группа подстановок $G < S_n$, $n > 1$, в которой любой отличный от единицы элемент имеет не более одной неподвижной точки, называется группой Фробениуса.

Примеры групп Фробениуса

- $D_n = \mathbb{Z}_n^+ \rtimes \langle h \rangle$, где $h: x \mapsto -x \pmod n$, n — нечетное
- $\text{AGL}(1, q) = \mathbb{F}_q^+ \rtimes \mathbb{F}_q^*$
- $K \rtimes \langle h \rangle$, где K — регулярная группа, h — автоморфизм K без неподвижных неединичных точек

Теорема

Пусть $A \in GL(n, 2^r)$ является МР-матрицей и имеет группу автоморфизмов $(G, 1)$, $G < S_n$ — транзитивная группа. Тогда в зависимости от четности n группа G может быть одного из следующих типов:

- ❶ n четное и G — регулярная группа;
- ❷ n нечетное и G — регулярная группа;
- ❸ n нечетное и $G = K \ltimes \langle h \rangle$ — группа Фробениуса, где K — регулярная абелева группа, а h — инволюция.

Теорема

Пусть $G < S_n$ — интранзитивная группа, $\Delta_1, \dots, \Delta_t$ — орбиты группы G , упорядоченные по убыванию мощности, и $(G, 1)$ — группа автоморфизмов МР-матрицы $A \in GL(n, 2^r)$. Тогда возможны три случая.

- ❶ Если $|\Delta_i| \geq 2$ для всех $i = 1, \dots, t$ и $n \equiv 0 \pmod{|G|}$, то G — полурегулярная группа.
- ❷ Если $|\Delta_i| \geq 2$ для всех $i = 1, \dots, t$ и $n \not\equiv 0 \pmod{|G|}$, то $G|_{\Delta_t}$ — группа Фробениуса, $G|_{\Delta_i}$ — регулярная группа при всех $i \in \{1, \dots, t-1\}$ и группы $G|_{\Delta_1}, G|_{\Delta_2}, \dots, G|_{\Delta_t}$ изоморфны.
- ❸ Если $|\Delta_t| = 1$, то $G|_{\Delta_i}$ — регулярная группа при всех $i \in \{1, \dots, t-1\}$.

Результаты экспериментов

Таблица: Число МР-матриц 8×8 в случайной выборке объема 10^6

Группа G	Число МР-матриц в выборке
$(\mathbb{Z}_2^3)^+$	152730
$(\mathbb{Z}_4 \times \mathbb{Z}_2)^+$	22406
$\mathbb{Z}_8^+$	20008
$\mathbb{Z}_7^+$	12655
D_4^+	1535
Q_8	1280

Таблица: Число МР-матриц 9×9 в случайной выборке объема 10^6

Группа G	Число МР-матриц в выборке
$(\mathbb{Z}_2^3)^+$	10067
$(\mathbb{Z}_3^2)^+ \rtimes \langle B \rangle$	4584
D_9	4127
$\mathbb{Z}_9^+$	5
$(\mathbb{Z}_3^2)^+$	2
$\mathbb{Z}_8^+$	1
$(\mathbb{Z}_4 \times \mathbb{Z}_2)^+$	1
Q_8	0

Эффективно реализуемые МР–матрицы

Таблица: Наилучшие параметры матриц 8×8 , построенных с использованием группы автоморфизмов $(G, 1)$, $G < S_8$

Группа G	v_1	c
Q_8	24	6
$\mathbb{Z}_8^+$	24	6
$\mathbb{Z}_7^+$	21	8
$(\mathbb{Z}_4 \times \mathbb{Z}_2)^+$	16	7
D_4^+	16	7
$(\mathbb{Z}_2^3)^+$	8	8

c — количество различных элементов в матрице

v_1 — количество единиц в матрице

Полученные результаты усиливают результаты Vaudenay S., Junod P. 2004; и аналогичны результатам Gupta K., Pandey S., Ray I. 2017.

Шаблон, полученный с использованием с группы автоморфизмов $(G, 1)$, где $G < S_8$ и $G \cong Q_8$

a_1	1	a_2	a_3	1	1	a_4	a_5
a_3	a_1	1	a_2	a_5	1	1	a_4
a_2	a_3	a_1	1	a_4	a_5	1	1
1	a_2	a_3	a_1	1	a_4	a_5	1
a_4	1	1	a_5	a_1	a_3	a_2	1
a_5	a_4	1	1	1	a_1	a_3	a_2
1	a_5	a_4	1	a_2	1	a_1	a_3
1	1	a_5	a_4	a_3	a_2	1	a_1

Таблица: Наилучшие параметры шаблонов 8×8 , построенных с использованием группы автоморфизмов $(G, 1)$, $G < S_9$

Группа G	v_1	c
Q_8	24	6
$\mathbb{Z}_8^+$	24	6
$\mathbb{Z}_9^+$	22	6
$(\mathbb{Z}_3^2)^+$	22	6
$(\mathbb{Z}_2^3)^+$	21	8
$(\mathbb{Z}_4 \times \mathbb{Z}_2)^+$	21	8
D_9	15	5
$(\mathbb{Z}_3^2 \rtimes \langle B \rangle)^+$	15	5

c — количество различных элементов в матрице

v_1 — количество единиц в матрице

Полученные результаты усиливают результаты Vaudenay S., Junod P. 2004; и аналогичны результатам Gupta K., Pandey S., Ray I. 2017.

Шаблон, полученный с использованием с группы автоморфизмов $(G, 1)$, где $G < S_9$ и $G \cong (\mathbb{Z}_3^2 \rtimes \langle B \rangle)^+$

a_1	1	1	a_2	a_3	a_4	a_3	a_2
1	a_1	1	a_4	a_2	a_2	a_4	a_3
1	1	a_1	a_3	a_4	a_3	a_2	a_4
a_4	a_3	a_2	1	1	a_4	a_2	a_3
a_2	a_4	a_3	a_1	1	a_3	a_4	a_2
a_4	a_2	a_3	a_3	a_2	a_1	1	1
a_3	a_4	a_2	a_4	a_3	1	a_1	1
a_2	a_3	a_4	a_2	a_4	1	1	a_1

Инвариантные подпространства

Определение

Подпространство $W < \mathbb{F}_2^n$ называется инвариантным относительно линейного преобразования $L \in GL(n, 2)$, если $(W)L = W$.

Инвариантные подпространства могут быть использованы в методе инвариантных подпространств.⁴

Определение

Пусть $H < S_n$ и $\{1, \dots, n\} = \Gamma_1 \cup \dots \cup \Gamma_k$ — разбиение на орбиты группы H . Будем говорить, что подпространство $W_H < \mathbb{F}_{2^r}^n$ является H – орбитальным, если $W_H = \langle e_{\Gamma_1}, \dots, e_{\Gamma_k} \rangle$, где

$$e_{\Gamma_i} = \sum_{s \in \Gamma_i} e_s, \quad i = 1, \dots, k.$$

H – орбитальные подпространства являются инвариантными относительно параллельного действия одинаковых s -боксов.

⁴G. Leander, M. Abdelraheem, H. AlKhzaimi, E. Zenner «A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack», 2011.

Утверждение

Пусть $A = (a_{i,j})$ — квадратная матрица порядка n над полем $\mathbb{F}_{2^r}$ имеет группу автоморфизмов $\text{Aut}(A) = \{(g, g) \mid g \in G\}$, $G < S_n$. Тогда любое H – орбитальное подпространство W_H , где $H < G$, является инвариантным для A , то есть $(W_H) A \subseteq W_H$.

Из работы Давыдова С. («Об инвариантных подпространствах матриц-циркулянтов и рекурсивных матриц», 2024) следует, что H -орбитальные подпространства исчерпывают все инвариантные подпространства МР-циркулянта порядка $n = 2^m$.

Случай циркулянта порядка $n \neq 2^m$

Пример

Пусть $\mathbb{F}_{24} = \mathbb{F}_2[x]/_{x^4+x+1}$, $\mathbb{F}_{24}^* = \langle \theta \rangle$, $\theta = [x]$. Рассмотрим МР-циркулянт A порядка 6

$$A = \text{Circ}(\theta^3 + \theta, \theta^3 + \theta, 1, \theta^3 + 1, \theta^2, \theta^3 + \theta^2 + 1).$$

Собственные подпространства, инвариантные относительно A , исчерпываются следующими подпространствами:

$$\begin{aligned} W_1 &= \langle e_{\{1,2,3,4,5,6\}} \rangle, \\ W_2 &= \langle e_{\{1,3,5\}}, e_{\{2,4,6\}} \rangle, \\ W_3 &= \langle e_{\{1,4\}}, e_{\{2,5\}}, e_{\{3,6\}} \rangle, \\ W_4 &= \langle e_{\{1,2,4,5\}}, e_{\{3,6\}} \rangle, \\ W_5 &= \langle e_{\{1,3,4,6\}}, e_{\{2,5\}} \rangle, \\ W_6 &= \langle e_{\{1,4\}}, e_{\{2,3,5,6\}} \rangle. \end{aligned}$$

Подпространства W_1, W_2, W_3 являются H -орбитальными.

Подпространства W_4, W_5, W_6 H -орбитальными не являются ни для какой подгруппы $H < G = \langle (1, 2, 3, 4, 5, 6) \rangle$, но каждый блок Γ_i в разбиениях является объединением орбит подгруппы H .

Спасибо за внимание!