5. *Antony M.* Discrete Mathematics of Neural Networks: Selected Topics. SIAM, Philadelphia, 2001.

УДК 621.391:519.7 DOI 10.17223/2226308X/12/59

MDS-МАТРИЦЫ, ПОСТРОЕННЫЕ С ПОМОЩЬЮ СОПРОВОЖДАЮЩИХ МАТРИЦ МНОГОЧЛЕНОВ И ПОДСТАНОВОЧНЫХ МАТРИЦ

О. Кой Пуэнте

Предлагается новый метод построения MDS-матриц порядка $k = 4, 6$ над полем GF(256), основанный на возведении в степень сопровождающих матриц некоторых многочленов и последующим сложением с подстановочной матрицей. Оценивается число операций сложения по модулю 2, необходимых для вычисления образов векторов при действии соответствующих линейных преобразований. Построенные матрицы представляют интерес для использования в шифрсистемах, ориентированных на низкоресурсную реализацию.

Ключевые слова: *MDS-матрицы, сопровождающие матрицы многочленов, подстановочные матрицы, конечные поля, низкоресурсная криптография, XOR-сложность.*

Введение

Пусть $Q = \mathrm{GF}(2^n) = \mathrm{GF}(2)[x]/g(x)$ — конечное поле из 2^n элементов, где $g(x)$ — неприводимый многочлен степени n над полем GF(2). Множество всех вектор-строк длины k над полем Q обозначим через Q^k, а множество всех матриц размера $k \times k$ над полем Q — через $Q_{k,k}$.

Определение 1 [1]. Показатель рассеивания ρ матрицы $A \in Q_{k,k}$ определяется равенством

$$\rho(A) = \min_{\mathbf{a} \neq \mathbf{0}} \{\mathrm{w}(\mathbf{a}) + \mathrm{w}(\mathbf{a}A)\},$$

где $\mathrm{w}(\mathbf{a})$ — вес Хэмминга вектора $\mathbf{a} \in Q^k$, то есть количество его ненулевых элементов.

Определение 2 [1, 2]. Матрица $A \in Q_{k,k}$ называется MDS-матрицей, если $\rho(A) = k + 1$.

Определение 3 [2]. Пусть $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1} + x^k \in Q[x]$. Матрица $S_f \in Q_{k,k}$, определённая равенством

$$S_f = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ a_0 & a_1 & a_2 & \cdots & a_{k-1} \end{pmatrix},$$

называется сопровождающей матрицей многочлена $f(x)$.

В [3] предложено оценивать сложность реализации линейного слоя в блочных шифрсистемах подсчётом количества вентилей XOR, необходимых для реализации

умножения элемента над полем. Показано, что, в отличие от распространённого мнения, элементы с высоким весом Хэмминга также могут иметь низкую сложность реализации. Будем использовать эту новую характеристику для расчёта сложности реализации линейного слоя.

Определение 4 [3]. XOR-сложностью элемента $\alpha \in Q$ в фиксированном базисе назовём количество операций XOR, необходимых для реализации умножения α на произвольный элемент $\beta \in Q$.

Пример 1 [3]. Пусть $\mathrm{GF}(2^3) = \mathrm{GF}(2)[x]/(x^3+x+1)$ и $\{1, \alpha, \alpha^2\}$ — базис пространства $\mathrm{GF}(2^3)$ над полем $\mathrm{GF}(2)$. Умножение элемента $\alpha^4 = \alpha \oplus \alpha^2$ на произвольный элемент $\beta = b_0 \oplus b_1\alpha \oplus b_2\alpha^2$, где $b_i \in \mathrm{GF}(2)$, имеет вид

$$(b_0 \oplus b_1\alpha \oplus b_2\alpha^2)(\alpha \oplus \alpha^2) = (b_0 \oplus b_2) \oplus (b_0 \oplus b_1)\alpha \oplus (b_0 \oplus b_1 \oplus b_2)\alpha^2.$$

Элемент $\alpha^4\beta$ можно отождествить с элементом из $\mathrm{GF}(2)^3$ вида

$$(b_0 \oplus b_2,\ b_0 \oplus b_1,\ b_0 \oplus b_1 \oplus b_2),$$

в котором есть четыре операции XOR. Таким образом, XOR-сложность элемента α^4 равна 4.

Будем обозначать XOR-сложность элемента $\alpha \in Q$ как $\mathsf{XOR}(\alpha)$. Нетрудно проверить, что $\mathsf{XOR}(0) = \mathsf{XOR}(1) = 0$. XOR-сложность строки с номером i матрицы $M = (m_{i,j})_{k\times k}$ можно найти по формуле [3]

$$\sum_{j=1}^{k} \mathsf{XOR}(m_{i,j}) + (l_i - 1)n,$$

где l_i — количество ненулевых элементов в i-й строке. Тогда можно определить XOR-сложность матрицы $M = (m_{i,j}) \in Q_{k,k}$ по формуле

$$\mathsf{XOR}(M) = \sum_{i=1}^{k}\sum_{j=1}^{k} \mathsf{XOR}(m_{i,j}) + n\sum_{i=1}^{k}(l_i - 1).$$

Пусть $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1} + x^k$ и $\{c_1, \ldots, c_s\}$ — множество всех различных ненулевых коэффициентов многочлена $f(x)$. В [4] показано, что

$$\mathsf{XOR}(S_f) = \sum_{j=1}^{s} \mathsf{XOR}(c_j) + (l_f - 1)n; \tag{1}$$

$$\mathsf{XOR}(S_f^r) = r \cdot \mathsf{XOR}(S_f) \tag{2}$$

для любого $r \in \mathbb{N}$, где l_f — количество ненулевых элементов в последней строке матрицы S_f.

1. Построение MDS-отображений

Определение 5. Будем говорить, что линейное отображение $L : Q^k \longrightarrow Q^k$, заданное по правилу

$$L(\mathbf{a}) = \mathbf{a} \cdot A_\gamma(L),$$

является MDS-отображением, если $\rho(A_\gamma(L)) = k + 1$, где $A_\gamma(L)$ — матрица линейного отображения L в фиксированном базисе γ пространства Q^k.

В шифрсистемах, ориентированных на низкоресурсную реализацию, существенное значение имеет XOR-сложность используемых криптографических примитивов. Нахождение MDS-отображений с небольшим значением данного параметра является актуальной проблемой.

Предложим способ построения MDS-отображений над полем $\mathrm{GF}(2^8)$ вида

$$\mathcal{L}^k_{f,P} : \mathbf{a} \mapsto \mathbf{a}(S_f^{3k/2} \oplus P)^{\mathrm{T}}, \tag{3}$$

где S_f — сопровождающая матрица многочлена $f(x) \in \mathrm{GF}(2^8)[x]$ степени k; P — подстановочная матрица порядка k. С целью эффективной реализации коэффициенты многочлена $f(x)$ выберем из множества $\{0, 1, \alpha, \alpha^{-1}, \alpha^2, \alpha^3\}$, где α — произвольный примитивный элемент поля $\mathrm{GF}(2^8)$.

Пусть $k = 4$, $\lambda_1(x) = x^4 + \alpha x^3 + \alpha$, $\lambda_2 = x^4 + \alpha^2 x^3 + \alpha^2$, $\lambda_3 = x^4 + \alpha x^3 + \alpha^{-1}$, $\lambda_4 = x^4 + \alpha^3 x^3 + \alpha^3$ и

$$P_1 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Тогда $\mathcal{L}^4_{\lambda_i,P_1}(\mathbf{a}) = \mathbf{a}(S^6_{\lambda_i} \oplus P_1)^{\mathrm{T}}$, $i = 1, \ldots, 4$.

Пусть Λ_i — линейное преобразование, осуществляемое регистром сдвига с характеристическим многочленом $\lambda_i(x)$, $i = 1, \ldots, 4$. Тогда действие отображения $\mathcal{L}^4_{\lambda_i,P_1}$ на вектор $\mathbf{a} = (a_0, a_1, a_2, a_3) \in \mathrm{GF}(2^8)^4$ можно схематично представить в виде рис. 1.

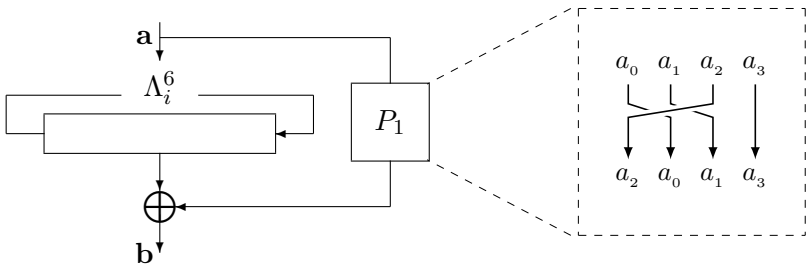

Рис. 1. Действие отображения $\mathcal{L}^4_{\lambda_i,P_1}$ при $i = 1, 2, 3, 4$

Теорема 1. Для любого $i = 1, \ldots, 4$ отображение $\mathcal{L}^4_{\lambda_i,P_1}$ является MDS-отображением.

Рассмотрим теперь отображения вида (3) в случае $k = 6$. Пусть $\alpha \in \mathrm{GF}(2^8)$ — корень многочлена $x^8 + x^7 + x^6 + x + 1$, $\tau_1(x) = x^6 + \alpha^{-1}x^5 + \alpha x^4 + \alpha$, $\tau_2(x) = x^6 + \alpha x^5 + {} + \alpha^{-1}x^4 + \alpha$, $\tau_3(x) = x^6 + \alpha^3 x^5 + x^4 + \alpha$, $\tau_4(x) = x^6 + \alpha^3 x^5 + x^4 + \alpha^{-1}$ и

$$P_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Тогда $\mathcal{L}^6_{\tau_i,P_2}(\mathbf{a}) = \mathbf{a}(S^9_{\tau_i} \oplus P_2)^{\mathrm{T}}$, $i = 1, \ldots, 4$.

Пусть T_i — линейное преобразование, осуществляемое регистром сдвига с характеристическом многочленом $\tau_i(x)$ для любого $i = 1, \ldots, 4$. Тогда действие отображения $\mathcal{L}^6_{\tau_i,P_2}$ на вектор $\mathbf{a} = (a_0, a_1, a_2, a_3, a_4, a_5) \in \mathrm{GF}(2^8)^6$ можно схематично представить в виде рис. 2.

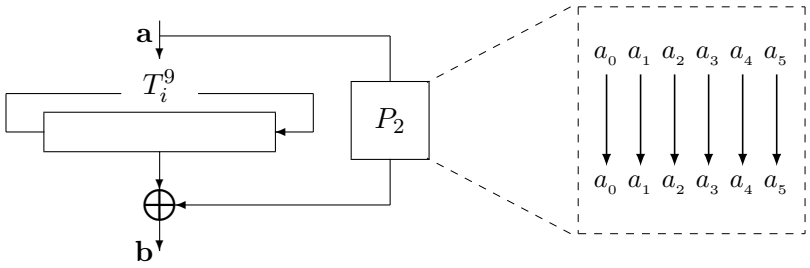

Рис. 2. Действие отображения $\mathcal{L}^6_{\tau_i,P_2}$ при $i = 1, \ldots, 4$

Теорема 2. Для любого $i = 1, \ldots, 4$ отображение $\mathcal{L}^6_{\tau_i,P_2}$ является MDS-отображением.

2. XOR-сложность некоторых MDS-отображений

Пусть $Q = \mathrm{GF}(2^8) = \mathrm{GF}(2)[x]/x^8 + x^7 + x^6 + x + 1$, θ — корень многочлена $x^8 + x^7 + x^6 + x + 1$. Записи табл. 1 соответствуют XOR-сложности элементов поля Q, заданных в шестнадцатеричном виде. Например, для элемента $\beta = \theta^5 + \theta^2 + \theta + 1 \in \mathrm{GF}(2^8)$ используется запись 0x27. Тогда $\mathsf{XOR}(\beta) = \mathsf{XOR}(\mathrm{0x27}) = 28$.

Таблица 1

XOR-сложность элементов поля Q

XOR	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f
0.	0	0	3	9	5	11	10	**14**	7	11	12	18	14	20	13	21
1.	12	18	11	19	13	17	18	**24**	17	23	22	26	12	20	23	29
2.	**16**	**22**	**21**	**25**	**11**	**19**	**22**	**28**	**17**	**23**	**16**	**24**	**18**	**22**	**23**	**29**
3.	20	24	25	31	27	33	26	**34**	11	19	22	28	24	30	29	33
4.	20	24	23	29	25	31	26	**34**	11	19	20	26	22	28	29	33
5.	18	24	25	29	15	23	24	**30**	19	25	20	28	22	26	25	31
6.	24	30	25	33	27	31	30	**36**	29	35	36	40	26	34	35	41
7.	10	18	19	25	21	27	28	**32**	25	29	28	34	30	36	31	39
8.	25	21	26	20	24	22	31	**27**	30	26	33	31	27	21	36	32
9.	11	5	20	16	22	18	25	**23**	22	20	29	25	31	27	32	26
a.	19	17	26	22	28	24	29	**23**	14	8	23	19	25	21	28	26
b.	21	17	24	22	18	12	27	**23**	22	18	23	17	21	19	28	24
c.	27	23	32	30	26	20	33	**29**	28	24	31	25	29	27	34	30
d.	31	29	36	32	38	34	41	**35**	26	20	33	29	35	31	40	38
e.	9	3	16	12	18	14	23	**21**	20	18	25	21	27	23	30	24
f.	25	21	28	22	26	24	31	**27**	30	26	35	33	29	23	36	32

Используя результаты из табл. 1, рассмотрим отображения из теорем 1 и 2. Для вычисления $\mathbf{a}(S^6_{\lambda_i})^{\mathrm{T}} \oplus \mathbf{a}(P_1)^{\mathrm{T}} = \mathbf{b}$ необходимо $4 \cdot 8 = 32$ операции XOR. Аналогично, для вычисления $\mathbf{a}(S^9_{\tau_i})^{\mathrm{T}} \oplus \mathbf{a}(P_2)^{\mathrm{T}} = \mathbf{b}$ необходимо $6 \cdot 8 = 48$ операций XOR. Тогда с помощью равенств (2) получим, что для пары

$$(f,P)=\begin{cases}(\lambda_i,P_1), & k=4,\\ (\tau_i,P_2), & k=6\end{cases}$$

справедливо равенство $\mathsf{XOR}(\mathcal{L}^k_{f,P})=\dfrac{3k}{2}\mathsf{XOR}(S_f)+8k$.

Пусть $h_1(x)=x^4+\beta^2x^3+x^2+\beta x+1$, $h_2(x)=x^4+(\beta+1)x^3+x^2+\beta x+1$, $h_3(x)=x^4+\beta^2x^3+x^2+x+\beta\in\mathrm{GF}(2^n)[x]$. В [5] показано, что при некоторых $\beta\in\mathrm{GF}(2^n)$ матрица $S^4_{h_i}$ является MDS-матрицей для любого $i=1,2,3$.

В работе [2] авторы использовали многочлены $g_1(x)=x^6+2x^5+8x^4+5x^3+8x^2+2x+1$ и $g_2(x)=x^6+4x^5+x^4+2x^3+x^2+3x+2$ для построения MDS-матриц размеров 6×6, используемых в семействе хэш-функции PHOTON, ориентированных на низкоресурсную реализацию. Они получили, что над полем $\mathrm{GF}(2^8)=\mathrm{GF}(2)[x]/x^8+x^4+x^3+x+1$ матрица $S^6_{g_i}$ является MDS-матрицей, $i=1,2$. Заметим, что среди многочленов вида

$$g'_1(x)=x^6+\beta x^5+\beta^3x^4+(\beta^2\oplus1)x^3+\beta^3x^2+\beta x+1,$$
$$g'_2(x)=x^6+\beta^2x^5+x^4+\beta x^3+x^2+(\beta\oplus1)x+\beta$$

для некоторого $\beta\in\mathrm{GF}(2^8)$ найдутся многочлены $g_1(x)$ и $g_2(x)$ соответственно.

С помощью значений из табл. 1 и равенств (1) и (2) при $\alpha=\beta=$ 0x02 получены результаты, приведённые в табл. 2 и 3. Из таблиц следует, что метод построения MDS-отображений на множествах Q^k при $k=4$ и 6, предложенный в данной работе, позволяет осуществить менее затратную реализацию, чем с использованием отображений из работ [2, 5].

Таблица 2

Сравнение параметра XOR-сложность для MDS-отображений множества Q^4

MDS-отображения	$S^4_{h_1}$	$S^4_{h_2}$	$S^4_{h_3}$	$\mathcal{L}^4_{\lambda_1,P_1}$	$\mathcal{L}^4_{\lambda_2,P_1}$	$\mathcal{L}^4_{\lambda_3,P_1}$	$\mathcal{L}^4_{\lambda_4,P_1}$
XOR-сложность	128	144	128	98	110	116	122

Таблица 3

Сравнение параметра XOR-сложность для MDS-отображений множества Q^6

MDS-отображения	$S^6_{g'_1}$	$S^6_{g'_2}$	$\mathcal{L}^6_{\tau_1,P_2}$	$\mathcal{L}^6_{\tau_2,P_2}$	$\mathcal{L}^6_{\tau_3,P_2}$	$\mathcal{L}^6_{\tau_4,P_2}$
XOR-сложность	366	342	246	246	282	282

Заключение

В работе предложен новый метод построения MDS-матрицы. Полученные MDS-матрицы обладают хорошими эксплуатационными характеристиками с точки зрения реализации на вычислительных платформах с ограниченными ресурсами.

ЛИТЕРАТУРА

1. *Augot D. and Finiasz M.* Direct construction of recursive MDS diffusion layers using shortened BCH codes // LNCS. 2014. V. 8540. P. 3–17.
2. *Guo J., Peyrin T., and Poschmann A.* The PHOTON family of lightweight hash functions // LNCS. 2011. V. 6841. P. 222–239.

3. *Sarkar S. and Sim S. M.* A deeper understanding of the XOR count distribution in the context of lightweight cryptography // LNCS. 2016. V. 9646. P. 167–182.
4. *Toh D., Teo J., Khoo K., and Sim S. M.* Lightweight MDS serial-type matrices with minimal fixed XOR count // LNCS. 2018. V. 10831. P. 51–71.
5. *Gupta K. C. and Ray I. G.* On constructions of MDS matrices from companion matrices for lightweight cryptography // LNCS. 2013. V. 8128. P. 29–43.

УДК 519.688 DOI 10.17223/2226308X/12/60

ВЫЧИСЛИТЕЛЬНЫЕ ЭКСПЕРИМЕНТЫ В КОНЕЧНЫХ ДВУПОРОЖДЁННЫХ БЕРНСАЙДОВЫХ ГРУППАХ ПЕРИОДА 5

А. А. Кузнецов

Пусть $B_0(2,5) = \langle a_1, a_2 \rangle$ — наибольшая конечная двупорождённая бернсайдова группа периода 5, порядок которой равен 5^{34}. Для каждого элемента данной группы существует единственное представление вида $a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot \ldots \cdot a_{34}^{\alpha_{34}}$, где $\alpha_i \in \mathbb{Z}_5$, $i = 1, 2, \ldots, 34$. Здесь a_1 и a_2 — порождающие элементы $B_0(2,5)$, $a_3, \ldots, a_{34}$ — коммутаторы, которые вычисляются рекурсивно через a_1 и a_2. Определим факторгруппу группы $B_0(2,5)$ следующего вида: $B_k = B_0(2,5)/\langle a_{k+1}, \ldots, a_{34} \rangle$. Очевидно, что $|B_k| = 5^k$. На основе проведённых вычислительных экспериментов сформулирована гипотеза о диаметре группы B_k для симметричного порождающего множества $\{a_1, a_1^{-1}, a_2, a_2^{-1}\}$.

Ключевые слова: *функция роста группы, группа Бернсайда.*

Настоящая работа продолжает исследования, начатые в [1, 2], которые посвящены разработке алгоритмов для исследования роста в конечных двупорождённых группах периода 5. В [1] основной упор сделан на создании алгоритмов минимальной вычислительной сложности, а в [2] разработан ресурсно-эффективный алгоритм, который имеет низкую пространственную сложность и сохраняет вычислительную сложность на приемлемом уровне.

Напомним основные определения [1]. Пусть $G = \langle X \rangle$. *Шаром* K_s радиуса s группы G будем называть множество всех её элементов, которые могут быть представлены в алфавите X в виде несократимых групповых слов длины не больше s. Все элементы одинаковой длины i образуют *сферу* P_i радиуса i. Единица группы e является пустым словом, длина которого равна нулю. Согласно данным определениям, $K_s = \bigcup\limits_{i=0}^{s} P_i$.

Для каждого целого неотрицательного i можно определить (сферическую) функцию роста группы $F(G)$, которую будем записывать в виде вектора $F(G) = (F_0, F_1, \ldots, F_i, \ldots)$, где $F_i = |P_i|$. Пусть $F_{s_0} > 0$, но $F_{s_0+1} = 0$, тогда s_0 является диаметром графа Кэли группы G в алфавите порождающих X, который будем обозначать $D_X(G)$. Средний диаметр $\overline{D}_X(G)$ равен $\dfrac{1}{|G|} \sum\limits_{s=0}^{s_0} sF_s$.

Заметим, что решение некоторых задач теории кодирования и криптографии сводится к исследованию соответствующих графов Кэли. Например, открытая проблема эффективного восстановления вершин в графе Хэмминга является одной из таких задач [3].

Кратко опишем алгоритмы из [1, 2].

Алгоритм 1 вычисляет шар K_s фиксированного радиуса s произвольной конечной группы G, заданной порождающим множеством X. Данный алгоритм имеет низкую