ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Апрель–июнь 2019. Т. 26, № 2. С. 115–128

УДК 519.688 DOI 10.33048/daio.2019.26.621

# ЭКСПЕРИМЕНТАЛЬНЫЕ МЕТОДЫ ПОСТРОЕНИЯ MDS МАТРИЦ СПЕЦИАЛЬНОГО ВИДА

*М. И. Рожков*[a], *С. С. Малахов*[b]

Национальный исследовательский университет
«Высшая школа экономики»,
ул. Мясницкая, 20, 101000 Москва, Россия

*E-mail:* [a]mirozhkov@hse.ru, [b]ssmalakhov@edu.hse.ru

**Аннотация.** MDS матрицы широко используются в качестве рассеивающего примитива при реализации итеративного метода построения преобразований блочного типа в связи с задачами защиты информации (алгоритмы AES, GOST 34.12-2015 и др.). При этом матрицы с большим числом единичных и малым числом различных элементов вызывают особый интерес с точки зрения эффективной реализации матрично-векторных умножений в условиях ресурсных ограничений. В настоящей работе описывается новый метод проверки признака MDS у матриц над конечным полем и демонстрируется его применение на примере матриц специального вида порядка $8 \times 8$, содержащих большое число единиц и малое число различных элементов. Такие матрицы были введены П. Юнодом и С. Воденеем. Для предложенного метода получены теоретические и экспериментальные оценки эффективности. Кроме того, в статье приводится список некоторых MDS матриц указанного вида. Табл. 7, библиогр. 15.

**Ключевые слова:** MDS матрица, MDS код.

## Введение

Рассмотрим матрицу $A = A_{r\times s}$ порядка $r \times s$ над конечным полем $\mathbb{F}_q = \mathrm{GF}(q)$. Тогда множество

$$\{(x, x \cdot A) \mid x \in (\mathbb{F}_q)^r\}$$

является линейным $(n, k, d)$ кодом с длиной кодового слова $n = r + s$ и размерностью $k = r$, а для его кодового расстояния справедлива оценка Синглтона $d \leqslant n - k + 1 = s + 1$. Если для указанного кода расстояние $d$ совпадает с верхней оценкой Синглтона, то код называется *MDS кодом*

(maximum distance separable); соответствующую матрицу $A$ называют *MDS матрицей*.

В связи с развитием методов разностного анализа (см. [1, 4, 5, 15]) данный тип матриц широко используется в области защиты информации для построения криптографических алгоритмов и хэш-функций (AES, Twofish, IDEA NXT (FOX), ГОСТ 34.12-2015 и др.). При этом матрицы с большим числом единичных и малым числом различных элементов, а также матрицы над полями $\mathrm{GF}(q) = \mathrm{GF}(2^t)$ вызывают особый интерес с точки зрения эффективной реализации матрично-векторных умножений в условиях ресурсных ограничений.

Методы построения MDS матриц рассматривались ранее многими авторами (см., например, [1, 7–14]). В [1, 7–9, 14] изучались MDS матрицы малого размера, в частности, $(4 \times 4)$-матрицы. В [10–13] исследовались MDS матрицы, являющиеся степенью сопровождающей матрицы. В [14] введено важное понятие би-регулярности матриц, связанное с невырожденностью её миноров размера $2 \times 2$. При этом для MDS матрицы свойство би-регулярности является необходимым. Кроме того, в [14] получены оценки для максимального числа единиц и минимального числа различных элементов в MDS матрицах заданного размера.

В настоящей работе исследуется новый метод, позволяющий проверять признак MDS у матриц, удовлетворяющих заранее известной структуре, который связан с предварительной символьной обработкой (классификацией) миноров матрицы и удалением повторов, а также миноров, отличающихся только знаком. Предложенный метод был применён к матрицам размера $8 \times 8$ двух типов, впервые введённых в [14]. Первый тип матриц содержит 21 единицу и 6 различных неединичных элементов. Второй тип содержит 15 единиц и 4 различных неединичных элементов. При этом, как известно [14], максимальное число единиц для MDS матриц размера $8 \times 8$ равно 24, а минимальное число различных неединичных элементов равно 4. Были получены теоретические и экспериментальные оценки вычислительной сложности предложенного метода, и с его помощью построены некоторые классы MDS матриц. Используемые в работе понятия из области конечных полей и линейных кодов приводятся в книгах [2, 3].

## 1. Описание метода

**Теорема 1** [3]**.** *Матрица $A$ является MDS матрицей, если и только если отличен от нуля каждый её минор.*

Теорема описывает необходимый и достаточный признак MDS матрицы — невырожденность всех её квадратных подматриц.

Пусть матрица $A$ удовлетворяет некоторому шаблону, а именно, элементы матрицы являются либо фиксированными элементами поля $\mathbb{F}_q$, либо неопределёнными переменными (символами) из множества независимых переменных $\{\alpha_1, \alpha_2, \ldots, \alpha_N\}$, $N \leqslant rs$. Тогда каждый её минор задаётся символьным выражением (многочленом) от соответствующих переменных. Обозначим через $D$ множество всех миноров матрицы $A$. Его мощность, очевидно, равна

$$|D| = \sum_{l=1}^{\min\{r,s\}} \binom{r}{l}\binom{s}{l}.$$

Через $D_2$, $D_2 \subseteq D$, обозначим наименьшее подмножество, для которого при любом миноре $m_i$ из множества $D$ существует минор $m_j$ из множества $D_2$ такой, что $m_i$ и $m_j$ совпадают как многочлены от символьных переменных матрицы над полем $\mathbb{F}_q$. Иными словами, $D_2$ получается из $D$ удалением дубликатов символьных выражений.

Через $D_1$, $D_1 \subseteq D_2 \subseteq D$, обозначим наименьшее подмножество множества $D_2$, для которого при любом миноре $m_i$ из множества $D_2$ существует минор $m_j$ из множества $D_1$ такой, что $m_i$ и $m_j$ как многочлены от символьных переменных матрицы над полем $\mathbb{F}_q$ совпадают с точностью до знака. Тем самым $D_1$ получается путём удаления из $D_2$ всех многочленов, для которых в $D_2$ найдутся многочлены, отличающиеся только знаком.

**Замечание 1.** Для полей $\mathrm{GF}(2^t)$ множества $D_1$ и $D_2$ совпадают.

**Замечание 2.** При заданных коэффициентах матрицы нулевые миноры в $D$, $D_1$ и $D_2$ присутствуют или отсутствуют одновременно. Таким образом, для проверки признака MDS достаточно убедиться в отсутствии нулевых миноров в множестве $D_1$.

**Определение 1.** Для произвольной матрицы $A$ (соответствующей рассматриваемому шаблону) назовём *контрольным множеством* любое множество её миноров, неравенство нулю которых эквивалентно наличию признака MDS у матрицы $A$.

Приведём неформальный алгоритм проверки признака MDS у матриц определённого выше шаблона. В этом алгоритме можно выделить две фазы: предварительную и проверочную.

**Предварительная фаза** (выделение контрольного множества)

Шаг 1. Построить множество всевозможных миноров матрицы рассматриваемого вида в общем символьном представлении.

Шаг 2. Найти и исключить из построенного на шаге 1 множества всевозможные миноры-дубликаты.

Шаг 3. Найти и исключить из построенного на шаге 2 множества всевозможные миноры, для которых найдётся в этом множестве другой минор, отличный только знаком.

**Проверочная фаза**

Шаг 4. Фиксируем элементами поля $\mathbb{F}_q$ символьные переменные матрицы и вычисляем значения миноров из контрольного множества.

Шаг 5. Если на предыдущем шаге найдётся нулевой минор, то соответствующая матрица не является MDS матрицей, в противном случае матрица будет MDS матрицей.

Во время первой фазы строится множество $D_1$, во время второй это множество используется в качестве контрольного и решается, является ли исследуемая матрица MDS матрицей.

Оценим сложность выделения контрольного множества для матрицы рассматриваемого типа. Пусть задана квадратная матрица размера $l \times l$, $l \leqslant \mu = \min\{r, s\}$, каждая клетка которой заполнена либо символьной переменной из множества $\{\alpha_1, \alpha_2, \ldots, \alpha_N\}$, либо конкретным элементом поля $\mathbb{F}_q$. Тогда её определитель как многочлен от переменных $\{\alpha_1, \alpha_2, \ldots, \alpha_N\}$ над полем $\mathbb{F}_q$ есть линейная комбинация мономов вида

$$(a_{1j_1})^{b_1} \times (a_{2j_2})^{b_2} \times \cdots \times (a_{N'j_{N'}})^{b_{N'}}, \tag{1}$$

где индексы и степени удовлетворяют соотношениям $N' \in \{1, 2, \ldots, N\}$, $1 \leqslant j_1 < j_2 < \cdots < j_{N'} \leqslant N$, $b_1 + b_2 + \cdots + b_{N'} \leqslant l$, $b_i > 0$.

Для оценки числа указанных мономов заметим, что при фиксированном $N'$ имеется $\binom{N}{N'}$ вариантов выбора $N'$ различных переменных из $N$ возможных. Тогда при фиксированной степени $B$ монома, $N' \leqslant B \leqslant l$, существует в точности $\binom{B-1}{N'-1}$ вариантов выбора $b_i$ таких, что $b_1 + b_2 + \cdots + b_{N'} = B$, так как это число совпадает с числом вариантов упорядоченных разбиений числа $B$ на $N'$ частей [6, разд. 4]. Следовательно, общее число мономов рассматриваемого вида равно

$$P(N, \mu) = \sum_{N'=1}^{N} \binom{N}{N'} \sum_{B=N'}^{\mu} \binom{B-1}{N'-1}.$$

Таким образом, каждый минор исходной матрицы $A_{r \times s}$ (как многочлен от символьных переменных) однозначно задаётся вектором длины $P(N, \mu)$ коэффициентов при соответствующих мономах. При этом поиск совпадающих миноров сводится к поиску совпадающих наборов коэффициентов.

Полагая сложность получения многочлена, соответствующего минору размера $l \times l$, равной $l!$ операций, сложность нахождения многочленов

для всех миноров размера $l \times l$ в матрице $A$ можно оценить величиной $\binom{\mu}{l}^2 \cdot l!$. Тогда сложность получения всех миноров матрицы $A$ составит

$$Q = \sum_{l=1}^{\mu} \binom{\mu}{l}^2 \cdot l!.$$

Далее, сложность удаления эквивалентных многочленов (дубликатов) можно оценить величиной

$$Q' = |D| \cdot (P(N, \mu) \cdot \frac{|D|}{|D_1|} + 2(|D| - |D_1|)).$$

При этом учитывалось, что для каждого многочлена из множества $D$ имеется в среднем (с учётом знака) $|D|/|D_1|$ дубликатов, для которых необходимо сравнение по всем коэффициентам соответствующих многочленов, т. е. $P(N, \mu)$ операций. Для остальных $|D| - |D_1|$ многочленов, которые отличны от исходного, требуется в среднем не более двух операций для сравнения коэффициентов.

Отметим, что при обработке большого числа матриц, удовлетворяющих заданному шаблону, время (сложность) предварительной работы $Q + Q'$ становится много меньше времени непосредственной проверки невырожденности миноров из контрольного множества.

Так как количество миноров, подлежащих вычислению, снижается в $|D|/|D_1|$ раз, для MDS матрицы снижение сложности проверки (ускорение) $S$ можно оценить величиной

$$S = \frac{\sum\limits_{m \in D} W(m)}{\sum\limits_{m \in D_1} W(m)},$$

где $W(m)$ — сложность вычисления минора $m$. Полагая сложность вычисления минора равной одной операции, для величины ускорения получим оценку $S = |D|/|D_1|$. Можно ожидать, что практическое ускорение обработки матрицы со случайным выбором элементов будет также близко к величине $S$.

Отметим также, что работа с минорами как многочленами необходима только на предварительном этапе при выделении контрольного подмножества и матрицы, соответствующие контрольному подмножеству, можно задавать не только набором коэффициентов при соответствующих мономах, но и указанием номеров строк и столбцов. В этом случае соответствующие миноры при фиксации символьных переменных элементами поля можно вычислять любым (наиболее эффективным) способом.

**Замечание 3.** Известно [2], что для поля $\mathbb{F}_q$, $q = p^i$, где $p$ — простое число, отображение

$$\varphi(x) = x^{p^t}, \quad x \in \mathbb{F}_q,\ t \in \{1, 2, \ldots, i\},$$

является автоморфизмом поля. Следовательно, миноры матриц $A$ и $\varphi(A)$ равны или не равны нулю одновременно. Кроме того, указанные матрицы обладают одинаковой структурой расположения единиц и пар различных элементов. Отмеченное свойство также можно использовать для снижения средней сложности экспериментальных методов построения MDS матриц.

## 2. Применение метода к матрицам специального вида

Рассмотрим над полем $\mathbb{F}_q$ матричный шаблон $A = M_6$ размера $8 \times 8$:

$$M_6 = \begin{pmatrix} f & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & a & b & c & d & e & f \\ 1 & f & 1 & a & b & c & d & e \\ 1 & e & f & 1 & a & b & c & d \\ 1 & d & e & f & 1 & a & b & c \\ 1 & c & d & e & f & 1 & a & b \\ 1 & b & c & d & e & f & 1 & a \\ 1 & a & b & c & d & e & f & 1 \end{pmatrix}.$$

Матрица данного типа была введена в рассмотрение в [14] и характеризуется одновременно большим числом единиц (их число 21 близко к верхней оценке $\vartheta \leqslant 24$) и малым числом различных неединичных элементов (их число 6 близко к нижней границе $c \geqslant 4$). Любой минор матрицы $M_6$ представляется символьным выражением (многочленом) от переменных $a$, $b$, $c$, $d$, $e$, $f$, и мощность множества всех миноров равна

$$|D| = \sum_{k=1}^{8} \binom{8}{k}^2 = 12869.$$

При этом для задания всех этих миноров требуется $P(6, 8) = 3002$ мономов вида (1). С помощью расчётов на ЭВМ были построены множества $D_1$ и $D_2$. При этом на построение множества $D_1$ потребовалось 6 секунд для поля $\mathbb{F}_q$ общего вида и 15 секунд при рассмотрении поля характеристики 2. Оценки числа миноров соответствующего порядка в данных множествах для полей $\mathrm{GF}(q)$ и, в частности, для $\mathrm{GF}(2^t)$ приведены табл. 1 и 2 соответственно.

*Таблица 1*

**Число миноров для поля** $\mathrm{GF}(q)$

| Порядок минора, $l$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | Общее число миноров |
|---|---|---|---|---|---|---|---|---|---|
| $\lvert D\rvert$ | 64 | 784 | 3136 | 4900 | 3136 | 784 | 64 | 1 | 12869 |
| $\lvert D_2\rvert$ | 7 | 129 | 396 | 661 | 458 | 730 | 63 | 1 | 2445 |
| $\lvert D_1\rvert$ | 7 | 68 | 252 | 385 | 252 | 693 | 63 | 1 | 1721 |

*Таблица 2*

**Число миноров для поля** $\mathrm{GF}(2^t)$

| Порядок минора, $l$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | Общее число миноров |
|---|---|---|---|---|---|---|---|---|---|
| $\lvert D\rvert$ | 64 | 784 | 3136 | 4900 | 3136 | 784 | 64 | 1 | 12869 |
| $\lvert D_1\rvert$ | 7 | 68 | 252 | 385 | 252 | 70 | 9 | 1 | 1044 |

*Таблица 3*

**Число миноров для поля** $\mathrm{GF}(q)$

| Порядок минора, $l$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | Общее число миноров |
|---|---|---|---|---|---|---|---|---|---|
| $\lvert D\rvert$ | 64 | 784 | 3136 | 4900 | 3136 | 784 | 64 | 1 | 12869 |
| $\lvert D_2\rvert$ | 5 | 89 | 432 | 897 | 818 | 784 | 64 | 1 | 3090 |
| $\lvert D_1\rvert$ | 5 | 50 | 224 | 485 | 484 | 766 | 64 | 1 | 2079 |

*Таблица 4*

**Число миноров для поля** $\mathrm{GF}(2^t)$

| Порядок минора, $l$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | Общее число миноров |
|---|---|---|---|---|---|---|---|---|---|
| $\lvert D\rvert$ | 64 | 784 | 3136 | 4900 | 3136 | 784 | 64 | 1 | 12869 |
| $\lvert D_1\rvert$ | 5 | 50 | 224 | 485 | 484 | 211 | 32 | 1 | 1492 |

Приведённые в табл. 1 и 2 результаты позволяют ожидать, что при использовании контрольного множества $D_1$ вычислительная сложность проверки признака MDS у матрицы $M_6$ при случайном выборе элементов $a$, $b$, $c$, $d$, $e$, $f$ снизится в $S \sim |D|/|D_1| = 7{,}5$ раз для поля $\mathbb{F}_q$ и в $S \sim 12{,}3$ раз для поля $\mathbb{F}_{2^t}$.

Аналогичные расчёты были проведены для матричного шаблона вида

$$A = M_4 = \begin{pmatrix} b & a & c & b & d & c & 1 & d \\ b & c & a & d & b & 1 & c & 1 \\ c & b & d & a & 1 & b & 1 & c \\ c & d & b & 1 & a & 1 & b & d \\ d & c & 1 & b & 1 & a & d & b \\ d & 1 & c & 1 & b & d & a & c \\ 1 & d & 1 & c & d & b & c & a \\ 1 & 1 & d & d & c & c & b & b \end{pmatrix}.$$

В этом случае для задания миноров требуется $P(4,8) = 494$ монома вида (1). При этом на построение множества $D_1$ потребовалось 6 секунд при рассмотрении матрицы над произвольным конечным полем и 11 секунд при рассмотрении над полем характеристики 2. Результаты расчётов приведены в табл. 3 и 4. Ожидаемая оценка ускорения принимает вид

$$\begin{cases} S \sim 6, & \text{если } \operatorname{char}(\mathbb{F}_q) \neq 2, \\ S \sim 8, & \text{если } \operatorname{char}(\mathbb{F}_q) = 2. \end{cases}$$

## 3. Экспериментальные исследования

Полученные результаты позволяют ожидать, что после выделения контрольного множества $D_1$ вычислительная сложность проверки признака MDS у матриц $M_6$ и $M_4$ при случайном выборе элементов из поля снизится в несколько раз. Для практической оценки уровня снижения сложности были проведены экспериментальные исследования для поля GF(256), которое рассматривалось как множество двоичных многочленов с операциями сложения и умножения по модулю неприводимого многочлена $h(x) = x^8 + x^6 + x^3 + x^2 + 1$.

Проверку признака MDS при использовании всех подматриц $D$ будем называть полной проверкой и обозначать соответствующее время через $T_{ft}$ (full testing). Проверку при использовании множества $D_1$ будем называть сокращённой проверкой и обозначать соответствующее ей время через $T_{st}$ (short testing). Экспериментальную оценку ускорения обозначим через $\widetilde{S}$, $\widetilde{S} = T_{ft}/T_{st}$.

Экспериментальные исследования проводились на ПЭВМ Intel Core i5-2400 CPU 3,10 GHz с использованием системы компьютерной алгебры Wolfram Mathematica 9.0. Были получены следующие результаты.

1. При исследовании матриц вида $M_6$ и $M_4$ со случайным выбором элементов из поля получено, что в среднем $T_{ft} = 197{,}8$ с, $T_{st} = 16{,}5$ с для матриц вида $M_6$; $T_{ft} = 150{,}1$ с, $T_{st} = 25{,}9$ с для матриц вида $M_4$. Итак, $\widetilde{S} = 12{,}0$ для $M_6$, $\widetilde{S} = 5{,}8$ для $M_4$. Полученные результаты подтверждают ожидаемое снижение времени проверки признака MDS для рассматриваемых матриц над полями характеристики 2.

2. Установлено, что не существует MDS матриц рассматриваемого вида, у которых степень элементов (как двоичных многочленов) не превосходит 2.

3. Найдены все MDS матрицы типа $M_4$, степень элементов которых не превосходит 3.

Имеется 14 двоичных многочленов, отличных от 0 и 1, степень которых не превосходит 3. Так как элементы $a$, $b$, $c$, $d$ MDS матрицы типа $M_4$ должны быть различны, имеется $14 \times 13 \times 12 \times 11 = 24024$ вариантов выбора указанных элементов. Аналогично для $M_6$ коэффициенты $a$, $b$, $c$, $d$, $e$, $f$ можно выбрать 2162160 способами. Занумеруем отличные от констант двоичные многочлены $g(x)$, $\deg(g) \leqslant 3$, в соответствии с табл. 5.

*Таблица 5*

**Соответствие полиномов и их кратких записей**

| | | | | | |
|---|---|---|---|---|---|
| $x$ | 2 | $1 + x + x^2$ | 7 | $x^2 + x^3$ | 12 |
| $1 + x$ | 3 | $x^3$ | 8 | $1 + x^2 + x^3$ | 13 |
| $x^2$ | 4 | $1 + x^3$ | 9 | $x + x^2 + x^3$ | 14 |
| $1 + x^2$ | 5 | $x + x^3$ | 10 | $1 + x + x^2 + x^3$ | 15 |
| $x + x^2$ | 6 | $1 + x + x^3$ | 11 | | |

В табл. 6 приведены все MDS матрицы типа $M_4$, задаваемые набором элементов $a$, $b$, $c$, $d$, степень которых (как двоичных многочленов) не превосходит 3. При этом время проверки признака MDS для всех 24024 вариантов соответствующих матриц составило 3,6 часов. В табл. 7 приведены примеры MDS матриц типа $M_6$, задаваемых набором элементов $a$, $b$, $c$, $d$, $e$, $f$ со степенью элементов, не превосходящей 3. Числа в табл. 6 и 7 следует понимать как краткие записи полиномов из табл. 5.

**Замечание 4.** Экспериментальными расчётами установлено, что все приведенные в табл. 6 и 7 матрицы являются MDS матрицами как для поля GF(256), так и для поля $\mathrm{GF}(2^{16})$, которое задаётся неприводимым двоичным многочленом $f(x) = x^{16} + x^{14} + x^{12} + x^7 + x^6 + x^4 + x^2 + x + 1$.

*Таблица 6*

**Перечень всех MDS матриц типа $M_4$ (с ограничением $\deg(g) \leqslant 3$ для элементов матриц)**

| | | | |
|---|---|---|---|
| 02, 04, 03, 15 | 05, 12, 11, 07 | 08, 06, 05, 13 | 12, 05, 15, 13 |
| 02, 04, 09, 12 | 05, 14, 11, 02 | 08, 09, 12, 07 | 12, 11, 02, 13 |
| 02, 13, 09, 05 | 06, 02, 14, 11 | 08, 10, 09, 14 | 12, 15, 11, 07 |
| 03, 08, 04, 09 | 06, 07, 09, 12 | 09, 05, 06, 12 | 13, 02, 09, 11 |
| 03, 08, 11, 04 | 06, 09, 04, 10 | 09, 08, 04, 14 | 13, 07, 12, 10 |
| 03, 11, 13, 10 | 06, 12, 09, 04 | 09, 11, 15, 12 | 13, 09, 15, 06 |
| 03, 12, 02, 07 | 06, 14, 03, 05 | 10, 08, 06, 14 | 13, 11, 15, 12 |
| 03, 13, 08, 14 | 06, 15, 02, 09 | 11, 03, 08, 14 | 14, 09, 15, 04 |
| 03, 13, 09, 06 | 07, 04, 10, 03 | 11, 05, 02, 06 | 15, 08, 07, 11 |
| 04, 02, 13, 10 | 07, 05, 11, 06 | 11, 08, 14, 05 | 15, 08, 11, 14 |
| 04, 12, 05, 02 | 07, 08, 02, 09 | 11, 10, 03, 13 | 15, 14, 03, 11 |
| 04, 15, 05, 08 | 07, 10, 13, 06 | 11, 12, 10, 14 | 15, 14, 06, 12 |

*Таблица 7*

**Перечень MDS матриц типа $M_6$ (с ограничением $\deg(g) \leqslant 3$ для элементов матриц)**

| | | | |
|---|---|---|---|
| 02, 03, 05, 13, 14, 08 | 02, 03, 09, 13, 04, 15 | 02, 03, 12, 06, 07, 15 | 02, 03, 15, 07, 10, 12 |
| 02, 03, 07, 12, 06, 10 | 02, 03, 10, 04, 09, 13 | 02, 03, 13, 04, 10, 06 | 02, 03, 15, 07, 11, 12 |
| 02, 03, 08, 04, 12, 07 | 02, 03, 10, 11, 06, 09 | 02, 03, 13, 10, 12, 09 | 02, 03, 15, 07, 12, 14 |
| 02, 03, 08, 04, 15, 13 | 02, 03, 10, 11, 07, 13 | 02, 03, 13, 15, 12, 09 | 02, 03, 15, 08, 10, 14 |
| 02, 03, 08, 09, 04, 12 | 02, 03, 10, 11, 12, 08 | 02, 03, 14, 11, 10, 05 | 02, 03, 15, 09, 06, 13 |
| 02, 03, 08, 14, 06, 15 | 02, 03, 11, 07, 04, 12 | 02, 03, 14, 15, 05, 08 | 02, 03, 15, 09, 07, 06 |
| 02, 03, 08, 14, 10, 06 | 02, 03, 11, 12, 06, 10 | 02, 03, 14, 15, 05, 12 | 02, 03, 15, 10, 13, 14 |
| 02, 03, 08, 14, 13, 15 | 02, 03, 11, 12, 08, 13 | 02, 03, 14, 15, 06, 10 | 02, 03, 15, 13, 04, 09 |
| 02, 03, 09, 06, 08, 15 | 02, 03, 11, 13, 10, 07 | 02, 03, 15, 06, 07, 13 | 02, 03, 15, 13, 11, 08 |
| 02, 03, 09, 08, 15, 12 | 02, 03, 11, 15, 12, 09 | 02, 03, 15, 07, 08, 14 | 02, 03, 15, 14, 04, 10 |

## Заключение

В работе исследован новый подход к снижению вычислительной сложности проверки признака MDS у матриц с заранее заданным матричным шаблоном.

Рассматриваемый метод предусматривает выделение из множества всех миноров $D$ контрольного подмножества $D_1$. При этом можно ожидать, что при использовании подмножества $D_1$ вычислительная сложность проверки признака MDS при случайном выборе элементов матрицы снизится в $S \sim |D|/|D_1|$ раз. Для двух типов матриц $M_6$ и $M_4$, введённых в [14] и имеющих размер $8 \times 8$, были построены подмножества $D_1$ и с целью оценки уровня снижения сложности были проведены экспериментальные исследования для поля GF(256). Эксперименты

показали, что практический уровень снижения сложности действительно соответствует ожидаемому теоретическому и составляет $k \sim 12$ раз для $M_6$ и $k \sim 6$ раз для $M_4$.

Кроме того, в работе получены все MDS матрицы типа $M_4$ над полем GF(256), у которых элементы (как двоичные многочлены) имеют степень не превышающую 3, а также приведены примеры таких матриц типа $M_6$. При необходимости могут быть построены MDS матрицы типов $M_6$ и $M_4$ и при других ограничениях на их элементы (например, малое число мономов в их представлении).

Рассмотренный в работе подход может быть эффективным и для других типов матриц (в том числе и большего размера) с малым числом различных элементов.

## ЛИТЕРАТУРА


1. **Анашкин А. В.** Полное описание одного класса MDS-матриц над конечным полем характеристики 2 // Мат. вопросы криптографии. 2017. Т. 8, № 4. С. 5–28.
2. **Лидл Р., Нидеррайтер Г.** Конечные поля. М.: Мир, 1988. 820 с.
3. **Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.** Теория кодов, исправляющих ошибки. М.: Связь, 1977. 744 с.
4. **Малышев Ф. М.** Двойственность разностного и линейного методов в криптографии // Мат. вопросы криптографии. 2014. Т. 5, № 3. С. 35–47.
5. **Малышев Ф. М., Трифонов Д. И.** Рассеивающие свойства XSLP-шифров // Мат. вопросы криптографии. 2016. Т. 7, № 3, С. 47–60.
6. **Холл М.** Комбинаторика. М.: Мир, 1970. 424 с.
7. **Augot D., Finiasz M.** Exhaustive search for small dimension recursive MDS diffusion layers for block ciphers and hash functions // Proc. IEEE Int. Symp. Information Theory (Istanbul, Turkey, July 7–12, 2013). Piscataway: IEEE, 2013. P. 1551–1555.
8. **Belov A. V., Los A. B., Rozhkov M. I.** Some approaches to construct MDS matrices over a finite field // Commun. Appl. Math. Comput. 2017. Vol. 31, No. 2. P. 143–152.
9. **Belov A. V., Los A. B., Rozhkov M. I.** Some classes of the MDS matrices over a finite field // Lobachevskii J. Math. 2017. Vol. 38, No. 5. P. 880–883.
10. **Couselo E., González S., Markov V., Nechaev A.** Recursive MDS-codes and recursive differentiable quasigroups // Discrete Math. Appl. 1998. Vol. 8, No. 3. P. 217–245.
11. **Couselo E., González S., Markov V., Nechaev A.** Parameters of recursive MDS-codes // Discrete Math. Appl. 2000. Vol. 10, No. 5. P. 433–453.
12. **Gupta K. C., Ray I. G.** On constructions of MDS matrices from companion matrices for lightweight cryptography // Security Engineering and Intelligence Informatics : Proc. CD-ARES 2013 Workshops (Regensburg, Germany, Sept. 2–6, 2013). Heidelberg: Springer, 2013. P. 29–43 (Lect. Notes Comp. Sci.; Vol. 8128).

**13. Gupta K. C., Ray I. G.** On constructions of circulant MDS matrices for lightweight cryptography // Information Security Practice and Experience : Proc. 10th Int. Conf. (Fuzhou, China, May 5–8, 2014). Cham: Springer, 2014. P. 564–576. (Lect. Notes Comput. Sci.; Vol. 8434).

**14. Junod P., Vaudenay S.** Perfect diffusion primitives for block ciphers: building efficient MDS matrices // Rev. Sel. Pap. 11th Int. Conf. Sel. Areas Cryptogr. (Waterloo, Canada, Aug. 9–10, 2004). Heidelberg: Springer, 2005. P. 84–99. (Lect. Notes Comput. Sci.; Vol. 3357).

**15. Matsui M.** On correlation between the order of S-boxes and the strength of DES // Advances in Cryptology – EUROCRYPT'94 : Proc. Workshop Theory Appl. Cryptogr. Tech. (Perugia, Italy, May 9–12, 1994). Heidelberg: Springer, 1995. P. 366–375. (Lect. Notes Comput. Sci.; Vol. 950).

*Рожков Михаил Иванович*
*Малахов Станислав Сергеевич*

Статья поступила
22 мая 2018 г.
После доработки —
28 января 2019 г.
Принята к публикации
29 января 2019 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
April–June 2019. Vol. 26, No. 2. P. 115–128

UDC 519.688 DOI 10.33048/daio.2019.26.621

# EXPERIMENTAL METHODS FOR CONSTRUCTING MDS MATRICES OF A SPECIAL FORM

*M. I. Rozhkov*[a] and *S. S. Malakhov*[b]

National Research University "Higher School of Economics",
20 Myasnitskaya Street, 101000 Moscow, Russia

*E-mail:* [a]mirozhkov@hse.ru, [b]ssmalakhov@edu.hse.ru

**Abstract.** MDS matrices are widely used as a diffusion primitive in the construction of block type encryption algorithms and hash functions (such as AES and GOST 34.12–2015). The matrices with the maximum number of units and minimum number of different elements are important for more efficient realizations of the matrix-vector multiplication. The article presents a new method for the MDS testing of matrices over finite fields and shows its application to the $(8 \times 8)$-matrices of a special form with many units and few different elements; these matrices were introduced by Junod and Vaudenay. For the proposed method we obtain some theoretical and experimental estimates of effectiveness. Moreover, the article comprises a list of some MDS matrices of the above-indicated type. Tab. 7, bibliogr. 15.

**Keywords:** MDS matrix, MDS code.

## REFERENCES

1. **A. V. Anashkin,** Complete description of a class of MDS-matrices over finite field of characteristic 2, *Mat. Vopr. Kriptogr.,* **8**, No. 4, 5–28, 2017 [Russian].
2. **R. Lidl** and **H. Niederreiter,** *Finite Fields,* Camb. Univ. Press, Cambridge, 1985. Translated under the title *Konechnye polya,* Mir, Moscow, 1988 [Russian].
3. **F. J. MacWilliams** and **N. J. A. Sloane,** *The Theory of Error-Correcting Codes,* North-Holland, Amsterdam, 1977 (North-Holland Math. Libr., Vol. 16). Translated under the title *Teoriya kodov, ispravlyayushchikh oshibki,* Svyaz', Moscow, 1979 [Russian].
4. **F. M. Malyshev,** The duality of differential and linear methods in cryptography, *Mat. Vopr. Kriptogr.,* **5**, No. 3, 35–47, 2014 [Russian].
5. **F. M. Malyshev** and **D. I. Trifonov,** Diffusion properties of XSLP-ciphers, *Mat. Vopr. Kriptogr.,* **7**, No. 3, 47–60, 2016 [Russian].
6. **M. Hall, Jr.,** *Combinatorial Theory,* Blaisdell, Waltham, MA, 1967. Translated under the title *Kombinatorika,* Mir, Moscow, 1970 [Russian].

7. **D. Augot** and **M. Finiasz,** Exhaustive search for small dimension recursive MDS diffusion layers for block ciphers and hash functions, *Proc. 2013 IEEE Int. Symp. Inf. Theory, Istanbul, Turkey, July 7–12, 2013,* pp. 1551–1555, IEEE, Piscataway, 2013.
8. **A. V. Belov, A. B. Los,** and **M. I. Rozhkov,** Some approaches to construct MDS matrices over a finite field, *Commun. Appl. Math. Comp.,* **31**, No. 2, 143–152, 2017.
9. **A. V. Belov, A. B. Los,** and **M. I. Rozhkov,** Some classes of the MDS matrices over a finite field, *Lobachevskii J. Math.,* **38**, No. 5, 880–883, 2017.
10. **E. Couselo, S. González, V. Markov,** and **A. Nechaev,** Recursive MDS-codes and recursive differentiable quasigroups, *Discrete Math. Appl.,* **8**, No. 3, 217–245, 1998.
11. **E. Couselo, S. González, V. Markov,** and **A. Nechaev,** Parameters of recursive MDS-codes, *Discrete Math. Appl.,* **10**, No. 5, 433–453, 2000.
12. **K. C. Gupta** and **I. G. Ray,** On constructions of MDS matrices from companion matrices for lightweight cryptography, in *Security Engineering and Intelligence Informatics* (Proc. CD-ARES 2013 Workshops: MoCrySEn SeCIHD, Regensburg, Germany, Sept. 2–6, 2013), pp. 29–43, Springer, Heidelberg, 2013 (Lect. Notes Comput. Sci., Vol. 8128).
13. **K. C. Gupta** and **I. G. Ray,** On constructions of circulant MDS matrices for lightweight cryptography, in *Information Security Practice and Experience,* (Proc. 10th Int. Conf., Fuzhou, China, May 5–8, 2014), pp. 564–576, Springer, Cham, 2014 (Lect. Notes Comput. Sci., Vol. 8434).
14. **P. Junod** and **S. Vaudenay,** Perfect diffusion primitives for block ciphers: Building efficient MDS matrices, *Selected Areas in Cryptography* (Rev. Sel. Pap. 11th Int. Conf., Waterloo, Canada, Aug. 9–10, 2004), pp. 84–99, Springer, Heidelberg, 2005 (Lect. Notes Comput. Sci., Vol. 3357).
15. **M. Matsui,** On correlation between the order of S-boxes and the strength of DES, *Advances in Cryptology – EUROCRYPT'94* (Proc. Workshop Theory Appl. Cryptogr. Tech., Perugia, Italy, May 9–12, 1994), pp. 366–375, Springer, Heidelberg, 1995 (Lect. Notes Comput. Sci., Vol. 950).


*Mikhail I. Rozhkov*
*Stanislav S. Malakhov*

Received May 22, 2018
Revised January 28, 2019
Accepted January 29, 2019