Math-Net.Ru

Общероссийский математический портал

А. В. Анашкин, Полное описание одного класса MDS-матриц над конечным полем характеристики 2, *Матем. вопр. криптогр.*, 2017, том 8, выпуск 4, 5–28

DOI: <https://doi.org/10.4213/mvk238>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 35.173.219.149

26 апреля 2023 г., 15:33:49

**Полное описание одного класса MDS-матриц над
конечным полем характеристики 2**

А. В. Анашкин

Лаборатории ТВП, Москва

Получено 20.IV.2017

Аннотация. Приводится полное описание множества MDS-матриц размера $n \times n$, $n > 3$, над полем $GF(2^t)$, $t > 1$, элементы которых принадлежат множеству $\{e, \alpha, \alpha^2\}$, где e — единица поля, $\alpha \neq 0, e$. Доказано, что при $n \geq 6$ таких матриц не существует. При $n = 4, 5$ указаны необходимые и достаточные условия существования MDS-матриц среди матриц с элементами из множества $\{e, \alpha, \alpha^2\}$.

Ключевые слова: MDS-отображение, MDS-матрица

**Complete description of a class of MDS-matrices over finite field
of characteristic 2**

A. V. Anashkin

TVP Laboratories, Moscow

Abstract. We give complete description of the set of $n \times n$ MDS-matrices, $n > 3$, over $GF(2^t)$, $t > 1$, with elements from the set $\{e, \alpha, \alpha^2\}$, where e is an identity element, $\alpha \neq 0, e$. It is proved that there are no such matrices if $n \geq 6$. For $n = 4, 5$ the necessary and sufficient conditions of existence of MDS-matrices consisting of elements e, α, α^2 are given.

Key words: MDS-mapping, MDS-matrix

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 4, pp. 5–28 (Russian)

© Академия криптографии Российской Федерации, 2017 г.

Введение

В криптографической литературе предлагаются и исследуются различные математические конструкции, которые могут быть использованы для синтеза криптографических примитивов, например блочных шифров или хэш-функций. Одним из таких математических объектов являются так называемые «MDS-отображения (Maximum Distance Separable)».

В [1] свойство «быть MDS-отображением» распространено с множества линейных отображений векторных пространств на произвольные отображения и доказан критерий наличия этого свойства.

Для линейных отображений свойство «быть MDS-отображением» тесно связано со свойством квадратных матриц «быть MDS-матрицей»; такие матрицы активно изучались в связи с исследованиями MDS-кодов. MDS-матрицы появились как составная часть порождающей матрицы MDS-кода (отечественный термин — *коды МДР* (разделимые коды с максимальным расстоянием) [2]). Так как термин «MDS-отображения» расширен на множество отображений не обязательно равномошных множеств [1], термин MDS-матрица будет использоваться нами для не обязательно квадратных матриц.

Использование MDS-матриц в качестве линейных преобразований при синтезе криптографических примитивов позволяет по сравнению с отображениями, не обладающими указанным свойством, вообще говоря, уменьшать максимальное число «благоприятных» нелинейных узлов, задействованных при построении как линейного, так и дифференциального соотношения для всего примитива, и тем самым обеспечивать большую стойкость как к линейному, так и к дифференциальному методу [3–10].

Практические соображения дают свои ограничения на вид MDS-матриц. К линейным отображениям предъявляются требования быстрой и простой как аппаратной, так и программной реализации. Особенно остро эта проблема возникает при синтезе так называемых *lightweight schemes* — схем, предназначенных для реализации на устройствах с ограниченными ресурсами.

Так, например, представляют интерес MDS-матрицы, у которых число единичных элементов по возможности велико, либо матрицы с минимальным числом различных элементов, либо матрицы, элементы которых являются степенями некоторого элемента, а показатели степеней имеют мало единиц в двоичной записи, и т. д. [11–16].

Кроме того (опять же с практической точки зрения), желательно иметь описание достаточно широкого класса «хороших» матриц. Это, во-первых, разнообразит спектр известных матриц, а во-вторых, предоставит разработчику криптографического алгоритма возможность выбора матрицы с нужными ему свойствами.

В данной работе для каждого $m \in \mathbb{N}$, $m \geq 4$, описано множество W_m всех квадратных MDS-матриц размера $m \times m$ над полем $GF(2^t)$, $t > 1$, элементы которых принадлежат множеству

$$D(\alpha) = \{e, \alpha, \alpha^2\}, \quad \alpha \in GF(2^t), \quad \alpha \neq e \text{ и } \alpha \neq 0.$$

Докажем, что если $m \geq 6$, то при любом α множество W_m является пустым. Также докажем, что при фиксированном элементе α множество W_5 состоит из матриц, получаемых всевозможными перестановками строк и столбцов одной матрицы, вид которой не зависит от значения α . При $m = 4$ (опять же с точностью до перестановки строк и столбцов) существует пять таких матриц, а с учетом дополнительной возможности транспонирования матрицы и замены $e \leftrightarrow \alpha^2$ элементов в матрице их всего две.

Умножение вектора на матрицу из множества W_m может быть достаточно эффективно реализовано как программно, так и аппаратно. В первом случае достаточно реализовать умножение элемента поля $GF(2^t)$ на элемент α . Во втором случае, представляя поле $GF(2^t)$ степенями сопровождающих матриц многочлена $f(x) \in GF(2)[x]$, корнем которого является элемент α , получаем малое число единиц в матрице линейного преобразования уже над полем $GF(2)$. Небольшое число единиц в матрице линейного преобразования, в свою очередь, позволяет обходиться малым числом логических элементов при его аппаратной реализации.

1. Определение MDS-матриц и их свойства

В приводимых определениях следуем работе [1]. Пусть A — произвольное непустое конечное множество. Для двух векторов $a = (\{a_1\}, \{a_2\}, \dots, \{a_n\})$, $b = (\{b_1\}, \{b_2\}, \dots, \{b_n\}) \in A^n$, $n \in \mathbb{N}$ (упорядоченных наборов из n элементов множества A) *расстоянием* между векторами a и b называется величина

$$\text{dist}(a, b) = |\{i \mid a_i \neq b_i, 1 \leq i \leq n\}|.$$

Пусть $n_1, n_2 \in \mathbb{N}$ и задано отображение $F: A^{n_1} \rightarrow A^{n_2}$. *Коэффициентом рассеивания* (в зарубежных работах — *branch number*) отображения F называется величина

$$\beta(F) = \min_{\substack{a, b \in A^{n_1}, \\ a \neq b}} \text{dist}((a, F(a)), (b, F(b))). \quad (1)$$

Так как $\text{dist}((a, F(a)), (b, F(b))) = \text{dist}(a, b) + \text{dist}(F(a), F(b))$, то

$$\begin{aligned}\beta(F) &\leq \min_{\substack{a, b \in A^{n_1}, \\ \text{dist}(a, b) = 1}} \text{dist}((a, F(a)), (b, F(b))) = \\ &= 1 + \min_{\substack{a, b \in A^{n_1}, \\ \text{dist}(a, b) = 1}} \text{dist}(F(a), F(b)) \leq 1 + n_2.\end{aligned}\tag{2}$$

Отображение $F: A^{n_1} \rightarrow A^{n_2}$ называется *MDS-отображением*, если $\beta(F) = 1 + n_2$, т. е. если на нем достигается оценка формулы (2). В [1] приведены необходимые и достаточные условия для того, чтобы отображение F было MDS-отображением: при любом s , $1 \leq s \leq \min(n_1, n_2)$, любая «редукция» (см. [1]) отображения F до преобразования множества A^s является биекцией.

Из указанного условия можно получить два следствия.

Пусть B — матрица размера $n_1 \times n_2$ над полем $GF(q^k)$, $q = p^t$, $t \in \mathbb{N}$, p — простое число. Коэффициентом рассеивания матрицы B называют число

$$\beta(B) = \min_{\substack{a \in GF(q^k)^{n_1}, \\ a \neq 0}} (w(a) + w(aB)),$$

где для вектора $x = (\{x_1\}, \{x_2\}, \dots, \{x_n\}) \in GF(q^k)^n$ через $w(x) = |\{i \mid x_i \neq 0, 1 \leq i \leq n\}|$ обозначается его вес Хемминга. Матрица B называется *MDS-матрицей*, если $\beta(B) = 1 + n_2$.

Утверждение 1. Матрица B размера $n_1 \times n_2$ над полем $GF(q^k)$, $q = p^t$, $t \in \mathbb{N}$, p — простое число, является MDS-матрицей тогда и только тогда, когда любая ее квадратная подматрица невырождена.

Утверждение 1 соответствует случаю, когда F — линейное отображение и множество A — конечное поле $GF(q^k)$, и является обобщением теоремы 8 (см. [2], стр. 312) на случай не обязательно квадратных матриц.

Утверждение 2. Пусть B — MDS-матрица размера $n_1 \times n_2$ над полем $GF(q^k)$, $q = p^t$, $t \in \mathbb{N}$, p — простое число. Любая матрица, полученная из матрицы B умножением любой ее строки или любого столбца на произвольный ненулевой элемент поля $GF(q^k)$, а также перестановкой любых ее двух строк или любых двух столбцов, также является MDS матрицей.

Утверждение 3. Любая подматрица MDS-матрицы также является MDS-матрицей.

З а м е ч а н и е. Не содержащие нулевых элементов вектор-строка и вектор-столбец являются MDS-матрицами.

Утверждение 4. Матрица B является MDS-матрицей тогда и только тогда, когда транспонированная матрица B^T является MDS-матрицей.

Утверждения 2–4 непосредственно вытекают из утверждения 1.

От матрицы линейного преобразования множества m -мерных векторов над полем $GF(q^k)$ можно однозначно, с точностью до выбора базиса векторного пространства $GF(q^k)_{GF(q)}$, перейти к матрице линейного преобразования множества $k \cdot m$ -мерных векторов над полем $GF(q)$. Поскольку в практических приложениях, как правило, используют преобразования векторов над меньшим полем $GF(q)$, то MDS-матрицу размера $m \times m$ над полем $GF(q^k)$ преобразуют (однозначно) в матрицу размера $k \cdot m \times k \cdot m$ над полем $GF(q)$.

Пусть F является линейным отображением, но теперь множество $A = GF(q)^k$ — это декартова степень поля $GF(q)$. Пусть $m \in \mathbb{N}$ и $n = k \cdot m$. Рассмотрим множество векторов размерности n над полем $GF(q)$. С учетом того, что $GF(q)^n = (GF(q)^k)^m = A^m$, представим $a \in GF(q)^n$ в виде

$$a = (a_1, a_2, \dots, a_k, a_{k+1}, \dots, a_n) = (a^{(1)}, a^{(2)}, \dots, a^{(m)}),$$

$$a^{(j)} = (a_{k \cdot (j-1) + 1}, a_{k \cdot (j-1) + 2}, \dots, a_{k \cdot (j-1) + k-1}, a_{k \cdot j}) \in GF(q)^k, \quad 1 \leq j \leq m.$$

Обобщенным (чтобы отличать от веса Хемминга) весом вектора a , согласованным с разбиением на подвекторы размерности k , называют величину $W(a) = |\{j \mid a^{(j)} \neq 0, 1 \leq j \leq m\}|$ [4].

Для матрицы B над полем $GF(q)$ размера $n_1 \times n_2$, $n_1 = k \cdot m_1$, $n_2 = k \cdot m_2$, коэффициентом рассеивания [4], согласованным с разбиением векторов на подвекторы размерности k , называют величину

$$\beta(B) = \min_{\substack{a \in GF(q)^{n_1}, \\ a \neq 0}} (W(a) + W(aB)).$$

Аналогично (2), для любой матрицы B верно неравенство $\beta(B) \leq 1 + m_2$. Матрицу B над полем $GF(q)$ размера $n_1 \times n_2$ ($n_1 = k \cdot m_1$, $n_2 = k \cdot m_2$), для которой выполняется равенство $\beta(B) = 1 + m_2$, называют матрицей с максимальным коэффициентом рассеивания или просто максимально рассеивающей матрицей [4].

Отметим еще раз, что для конкретной матрицы как значение ее коэффициента рассеивания β , так и свойство матрицы «быть максимально рассеивающей» зависят от параметра — разбиения векторов на подвекторы [3].

Для матрицы B над полем $GF(q)$ размера $n_1 \times n_2$ ($n_1 = k \cdot m_1$, $n_2 = k \cdot m_2$), для произвольного числа s ($1 \leq s \leq \min(m_1, m_2)$) и двух наборов чисел $1 \leq i_1 < i_2 < \dots < i_s \leq m_1$ и $1 \leq j_1 < j_2 < \dots < j_s \leq m_2$ определим ее квадратную подматрицу $B(s; i_1, \dots, i_s, j_1, \dots, j_s)$ размера $k \cdot s \times k \cdot s$, стоящую на пересечении строк с номерами

$i_1(k-1) + 1, i_1(k-1) + 2, \dots, i_1 k, i_2(k-1) + 1, i_2(k-1) + 2, \dots, i_s k$
и столбцов с номерами

$j_1(k-1) + 1, j_1(k-1) + 2, \dots, j_1 k, j_2(k-1) + 1, j_2(k-1) + 2, \dots, j_s k.$

Утверждение 5. Матрица B над полем $GF(q)$ размера $n_1 \times n_2$, $n_1 = k \cdot m_1$, $n_2 = k \cdot m_2$, является максимально рассеивающей тогда и только тогда, когда для любого числа s , $1 \leq s \leq \min(m_1, m_2)$, и любых двух наборов чисел $1 \leq i_1 < i_2 < \dots < i_s \leq m_1$ и $1 \leq j_1 < j_2 < \dots < j_s \leq m_2$ матрица $B(s; i_1, \dots, i_s, j_1, \dots, j_s)$ является обратимой.

З а м е ч а н и е. Утверждение 5 является следствием теоремы 2.9 [1], но не следует из теоремы 8 на стр. 312 в [2].

Далее рассматриваем случай $m_1 = m_2 = m$, $n_1 = n_2 = n$ как наиболее востребованный в практических приложениях.

2. Некоторые свойства MDS-матриц над полем

$GF(2^t)$, $t \geq 2$

Для непустого множества $D \subseteq GF(2^t)$, $m_1, m_2 \in \mathbb{N}$, рассмотрим множество таких матриц $G(D, m_1, m_2)$ над полем $GF(2^t)$ размера $m_1 \times m_2$, что все их элементы принадлежат множеству D .

Утверждение 6. Пусть $D = \{\alpha, \beta\}$, $\alpha \cdot \beta \neq 0$, $\alpha \neq \beta$ и матрица B принадлежит $G(D, m_1, m_2)$. Если B является MDS-матрицей и $m_1 = 2$, то $m_2 \leq 3$. Аналогично, если B является MDS-матрицей и $m_2 = 2$, то $m_1 \leq 3$.

Доказательство. Пусть $B \in G(D, 2, m_2)$. Если B является MDS-матрицей, то все ее столбцы попарно различны. Столбцы могут принимать всего 4 значения: $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \begin{pmatrix} \beta \\ \alpha \end{pmatrix}, \begin{pmatrix} \alpha \\ \alpha \end{pmatrix}, \begin{pmatrix} \beta \\ \beta \end{pmatrix}$. При этом в матрице B не могут одновременно содержаться столбцы 3 и 4, так как они линейно зависимы. Следовательно, $m_2 \leq 3$. Отметим, что верхняя граница является достижимой, поскольку определители всех подматриц размера 2×2 матрицы $\begin{pmatrix} \alpha & \beta & \alpha \\ \beta & \alpha & \alpha \end{pmatrix}$ не равны нулю, и, значит, эта матрица является MDS-матрицей. Вторая часть следует из утверждения 4. Утверждение доказано. $\square$

Следствие 1. Пусть B — MDS-матрица над полем $GF(2^t)$, содержащая подматрицу, элементы которой могут принимать всего два значения и один размер которой равен 2. Тогда второй размер подматрицы не превосходит 3.

Для элемента $\alpha \in GF(2^t) \setminus \{0, e\}$ везде далее через $D(\alpha)$ обозначаем множество $D(\alpha) = \{e, \alpha, \alpha^2\}$.

Множество $G(D(\alpha), 2, 1)$ имеет мощность 9 и является объединением четырех множеств:

$$\begin{aligned} G_0 &= \left\{ \begin{pmatrix} \alpha^2 \\ e \end{pmatrix}, \begin{pmatrix} e \\ \alpha^2 \end{pmatrix} \right\}, \quad G_1 = \left\{ \begin{pmatrix} e \\ \alpha \end{pmatrix}, \begin{pmatrix} \alpha \\ \alpha^2 \end{pmatrix} \right\}, \\ G_2 &= \left\{ \begin{pmatrix} \alpha \\ e \end{pmatrix}, \begin{pmatrix} \alpha^2 \\ \alpha \end{pmatrix} \right\}, \quad G_3 = \left\{ \begin{pmatrix} e \\ e \end{pmatrix}, \begin{pmatrix} \alpha \\ \alpha \end{pmatrix}, \begin{pmatrix} \alpha^2 \\ \alpha^2 \end{pmatrix} \right\}. \end{aligned}$$

В множестве $G(D(\alpha), 2, 2)$ выделим подмножество, обозначаемое далее через Z . Матрица принадлежит Z , если оба ее столбца либо совпадают, либо одновременно принадлежат одному из множеств G_1 , G_2 или G_3 . Определители матриц из множества Z равны нулю, следовательно, эти матрицы не являются MDS-матрицами. Матрицы из Z будем называть *запретами*.

З а м е ч а н и е. Определитель матрицы $\begin{pmatrix} \alpha^2 & e \\ e & \alpha \end{pmatrix}$ может быть равен нулю, если α — корень многочлена $x^2 + x + e$.

Утверждение 7. При $m_1 \geq 2$, $m_2 \geq 2$ MDS-матрица $B \in G(D(\alpha), m_1, m_2)$ не содержит подматриц размера 2×2 , являющихся запретами.

Доказательство является очевидным следствием утверждения 1.

Следствие 2. В множестве вектор-столбцов длины 2, полученных из любых двух строк MDS-матрицы $B \in G(D(\alpha), m_1, m_2)$ при $m_1 \geq 2$, $m_2 \geq 2$ содержится не более одного элемента каждого из множеств G_1 , G_2 и G_3 .

Утверждение 8. Любая матрица $B \in G(D(\alpha), 2, 2) \setminus Z$ является MDS-матрицей тогда и только тогда, когда степень минимального многочлена элемента α не меньше 3.

Для доказательства утверждения 8 достаточно вычислить определители всех матриц, не являющихся запретами. Нетрудно проверить, что множество значений определителей не содержит нуль тогда и только тогда, когда одновременно выполняются условия $\alpha \neq 0$, $\alpha \neq e$ и $\alpha^2 + \alpha + e \neq 0$ (здесь мы воспользовались тем, что $t > 1$ и характеристика поля равна 2). Выполнение этих условий равносильно тому, что степень минимального многочлена α не меньше 3.

З а м е ч а н и е. Условия утверждения 8 выполняются лишь в случае $t > 2$.

Утверждение 9. Если матрица $B \in G(D(\alpha), 2, m)$ является MDS-матрицей над полем $GF(2^t)$, то $m \leq 5$.

Доказательство. Пусть B является MDS-матрицей. Тогда множество ее столбцов содержит не более одного элемента каждого из множеств G_1 , G_2 или G_3 и любое количество элементов множества G_0 , $|G_0| = 2$. Следовательно, выполняется неравенство $m \leq 5$. $\square$

Следствие 3. Если B — MDS-матрица над полем $GF(2^t)$, элементы которой принадлежат множеству $D(\alpha)$, $\alpha \neq 0$ и $\alpha \neq e$, и один из ее размеров не меньше 2, то второй ее размер не превосходит 5.

Следствие 4. Если B — квадратная MDS-матрица над полем $GF(2^t)$ размера $m \times m$, элементы которой принадлежат множеству $D(\alpha)$, $\alpha \neq 0$ и $\alpha \neq e$, то $m \leq 5$.

Утверждение 10. Пусть $B \in G(D(\alpha), m_1, m_2)$, $2 \leq m_1, m_2 \leq 5$, B — MDS-матрица. Тогда в каждой строке и в каждом столбце матрицы B элемент α встречается не более трех раз. Если дополнительно выполняются либо условия $m_1 \geq 3$ и $m_2 \geq 4$, либо условия $m_1 \geq 4$ и $m_2 \geq 3$, то в каждой строке и в каждом столбце матрицы B элемент α встречается не более двух раз.

Доказательство. С учетом утверждения 2 можно переставлять строки и столбцы матрицы B нужным образом, не изменяя свойство матрицы быть MDS-матрицей. Кроме этого, доказательство будем проводить только в отношении столбцов. Утверждение для строк будет следовать из доказанного и из утверждения 4.

1. Предположим противное, т. е. что в некотором столбце матрицы B элемент α встретился хотя бы четыре раза. Переставим строки и столбцы матрицы так, чтобы она приняла вид

$$B = \begin{pmatrix} \alpha & X & \dots \\ \alpha & X & \dots \\ \alpha & X & \dots \\ \cdot & \cdot & \dots \end{pmatrix},$$

здесь и далее X — некоторые произвольные элементы из множества $D(\alpha)$. Рассмотрим элементы в столбце с номером 2 и в строках с номерами с 1 по 4.

Так как для каждого элемента имеется всего три возможных значения, то какие-то два элемента совпадают. Пусть, например, это будут элементы в первом и во втором столбцах: тогда подматрица матрицы B , стоящая на пересечении первой и второй строк и первого и второго столбцов, является запретом. Полученное противоречие показывает, что в каждом столбце матрицы B не может быть более трех элементов α .

Далее в доказательствах фразу «в подматрице матрицы B , расположенной на пересечении строк с номерами i_1 и i_2 и столбцов с номерами j_1 и j_2 , находится запрет» будем записывать так: $(i_1, i_2; j_1, j_2) \rightarrow Z$.

2. Пусть есть дополнительные условия на размеры матрицы. Предположим, что в некотором столбце матрицы есть три элемента α . Перестановкой строк и столбцов переместим их в первый столбец и первые три строки.

2.1 $m_1 \geq 3$ и $m_2 \geq 4$.

Рассмотрим подматрицу матрицы B , стоящую на пересечении первых трех строк и первых четырех столбцов, также являющуюся MDS-матрицей:

$$\begin{pmatrix} \alpha & X & X & X \\ \alpha & X & X & X \\ \alpha & X & X & X \end{pmatrix}.$$

В каждом столбце, кроме первого, элементы должны быть различными, иначе, как и в п.1, существовала бы матрица-запрет. Перестановкой строк получим:

$$\begin{pmatrix} \alpha & e & X & X \\ \alpha & \alpha & X & X \\ \alpha & \alpha^2 & X & X \end{pmatrix}.$$

Рассмотрим первые две строки. Заметим, что в этих строках первый столбец принадлежит множеству G_3 , а второй — G_1 . Если в одном из двух последних столбцов стоит вектор $\begin{pmatrix} \alpha^2 \\ e \end{pmatrix}$ из множества G_0 , то матрица принимает вид

$$\begin{pmatrix} \alpha & e & \alpha^2 & X \\ \alpha & \alpha & e & X \\ \alpha & \alpha^2 & \alpha & X \end{pmatrix}$$

и $(2, 3; 2, 3) \rightarrow Z$. Следовательно, на пересечении первых двух строк и столбцов с номерами 3 и 4 может стоять по одному вектору из множеств G_0 и G_2 , причем из множества G_0 — это вектор $\begin{pmatrix} e \\ \alpha^2 \end{pmatrix}$:

$$\begin{pmatrix} \alpha & e & e & X \\ \alpha & \alpha & \alpha^2 & X \\ \alpha & \alpha^2 & \alpha & X \end{pmatrix}.$$

Далее, рассмотрим строки с номерами 2 и 3. Первые три столбца в них — это векторы из множеств G_3 , G_1 и G_2 соответственно. Значит, столбец с номером 4 должен быть из множества G_0 , а тогда $b_{14} = \alpha$. Для матрицы $\begin{pmatrix} \alpha & e & e & \alpha \\ \alpha & \alpha & \alpha^2 & e \\ \alpha & \alpha^2 & \alpha & \alpha^2 \end{pmatrix}$ имеем запрет $(1, 3; 3, 4) \rightarrow Z$, а для матрицы $\begin{pmatrix} \alpha & e & e & \alpha \\ \alpha & \alpha & \alpha^2 & \alpha^2 \\ \alpha & \alpha^2 & \alpha & e \end{pmatrix}$ — запрет $(1, 2; 2, 4) \rightarrow Z$.

Во всех рассмотренных вариантах получили противоречие со свойством исходной матрицы быть MDS-матрицей. Таким образом, при выполнении условия п. 2.1 число элементов α в любом столбце матрицы не превосходит 2.

2.2 $m_1 \geq 4$ и $m_2 \geq 3$.

Аналогично рассматриваем подматрицу размера 4×3 матрицы B , которая является MDS-матрицей и имеет следующий вид:

$$\begin{pmatrix} \alpha & e & X \\ \alpha & \alpha & X \\ \alpha & \alpha^2 & X \\ X & X & X \end{pmatrix}.$$

Транспонированием приводим ее к виду $\begin{pmatrix} \alpha & \alpha & \alpha & X \\ e & \alpha & \alpha^2 & X \\ X & X & X & X \end{pmatrix}$, при этом первые три столбца в первых двух строках — это элементы множеств G_2 , G_3 и G_1 соответственно, значит, последний столбец в этих строках должен быть из множества G_0 . Аналогично получаем, что последний столбец в строках с номерами 1 и 3 должен быть из множества G_0 . А тогда последний столбец всей подматрицы может быть только двух видов: $\begin{pmatrix} e \\ \alpha^2 \\ \alpha^2 \end{pmatrix}$ или $\begin{pmatrix} \alpha^2 \\ e \\ e \end{pmatrix}$.

Как и в п.1, замечаем, что элементы строки с номером 3, стоящие в столбцах с номерами с 1 по 3, должны быть попарно различны. Если хотя бы для одного $j \in \{1, 2, 3\}$ выполняется равенство $b_{2j} = b_{3j}$, то $(2, 3; j, 4) \rightarrow Z$. Следовательно, $b_{2j} \neq b_{3j}$, $j = 1, 2, 3$. Тогда перестановкой строк и столбцов подматрицу можно привести к виду $\begin{pmatrix} \alpha & \alpha & \alpha & y \\ e & \alpha & \alpha^2 & z \\ \alpha & \alpha^2 & e & z \end{pmatrix}$, где $\{y, z\} = \{e, \alpha^2\}$. Тогда $(2, 3; 1, 2) \rightarrow Z$. Таким образом, в п. 2.2 также получаем противоречие с предположением.

В обоих рассмотренных вариантах получили противоречие со свойством исходной матрицы быть MDS-матрицей. Таким образом, при выполнении либо условия $m_1 \geq 3$ и $m_2 \geq 4$, либо условия $m_1 \geq 4$ и при выполнении $m_2 \geq 3$ число элементов α в любом столбце матрицы не превосходит 2.

Утверждение 10 доказано. $\square$

Пусть B — квадратная MDS-матрица над полем $GF(2^t)$ размера $m \times m$, элементы которой принадлежат множеству $D(\alpha)$, $\alpha \neq 0$ и $\alpha \neq e$. При $m = 1$ описание таких матриц тривиально, при $m = 2$ такие матрицы описаны в утверждении 8. В случае когда $m = 3$, не удастся достаточно просто перечислить все матрицы. В следующих двух утверждениях укажем два подкласса.

Утверждение 11. Пусть $B \in G(D(\alpha), 3, 3)$, B — MDS матрица, одна строка или один столбец которой состоит из одинаковых элементов. Тогда указанными в утверждении 2 преобразованиями матрицу B можно привести к виду

$$\begin{pmatrix} x & x & x \\ x & y & z \\ x & z & y \end{pmatrix},$$

где $\{x, y, z\} = D(\alpha)$.

Доказательство. По утверждению 4 можно ограничиться рассмотрением случая, когда в матрице B есть строка из одинаковых элементов.

По утверждению 2 матрицу можно B привести к виду $\begin{pmatrix} x^* & x^* & x^* \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix}$, где $x^* \in D(\alpha)$. Во второй строке должны встретиться все элементы из $D(\alpha)$, иначе в первой и второй строках будет запрет. Аналогично и в третьей строке должны встретиться все элементы из $D(\alpha)$.

Далее, вторая и третья строки не могут совпадать и не могут отличаться друг от друга циклическим сдвигом, поскольку в обоих случаях в них будет запрет. Значит, перестановкой столбцов матрицу B можно привести к виду $\begin{pmatrix} x^* & x^* & x^* \\ x & y & z \\ x & z & y \end{pmatrix}$. Умножая первую строку на $x \cdot (x^*)^{-1}$, получаем требуемый вид матрицы.

Утверждение 11 доказано. $\square$

Утверждение 12. Пусть $B \in G(D(\alpha), 3, 3)$, B — MDS-матрица. Если число различных элементов в матрице B равно 2, то перестановкой строк и столбцов матрицу B можно привести к виду

$$\begin{pmatrix} x & y & y \\ y & x & y \\ y & y & x \end{pmatrix}, \quad (3)$$

где $\{x, y\} \in D(\alpha)$, $x \neq y$.

Обратно, любая 3×3 матрица вида (3) при $x, y \in GF(2^t) \setminus \{0\}$, $x \neq y$, является MDS-матрицей.

Доказательство. Если хотя бы одна строка (или один столбец) матрицы B состоит из одинаковых элементов, то остальные строки (столбцы) должны состоять из различных элементов каждая (каждый), что противоречит условию. Следовательно, в каждой строке и в каждом столбце встречаются оба элемента.

Рассмотрим первую строку матрицы: элемент, который встречается в ней один раз, обозначим через x , а другой — через y . Перестановкой столбцов приведем ее к виду $\begin{pmatrix} x & y & y \\ . & . & . \\ . & . & . \end{pmatrix}$ и перестановкой строк — к виду $\begin{pmatrix} x & y & y \\ y & . & . \\ . & . & . \end{pmatrix}$.

Один из элементов b_{22} и b_{23} должен быть равен x . Оба элемента не могут быть равными x , поскольку тогда $(1, 2; 2, 3) \rightarrow Z$. Следовательно, по доказанному второй элемент равен y . Тогда перестановкой столбцов матрицу можно привести к виду $\begin{pmatrix} x & y & y \\ y & x & y \\ . & . & . \end{pmatrix}$.

Элемент b_{33} опять же по доказанному может быть равен только x : $\begin{pmatrix} x & y & y \\ y & x & y \\ . & . & x \end{pmatrix}$. Если элемент b_{32} равен x , то $(1, 3; 2, 3) \rightarrow Z$. Следовательно, $b_{32} = y$: $\begin{pmatrix} x & y & y \\ y & x & y \\ . & y & x \end{pmatrix}$. Если элемент b_{31} равен x , то $(2, 3; 1, 3) \rightarrow Z$. Следовательно, $b_{31} = y$: $\begin{pmatrix} x & y & y \\ y & x & y \\ y & y & x \end{pmatrix}$.

Далее, множество значений определителей всех подматриц размера 2×2 есть $\{(x+y)^2, y(x+y)\}$ и не содержит нуля, если $\{x, y\} \in GF(2^t) \setminus \{0\}$, $x \neq y$.

Определитель всей матрицы есть $x(x+y)^2$ и также не равен нулю, если $\{x, y\} \in GF(2^t) \setminus \{0\}$, $x \neq y$.

Утверждение 12 доказано. $\square$

Пример 1. Матрица $B = \begin{pmatrix} e & \alpha & \alpha^2 \\ e & \alpha^2 & \alpha \\ \alpha^2 & e & e \end{pmatrix}$, $\alpha \in GF(2^t) \setminus \{0, e\}$ и $\alpha^2 + \alpha + 1 \neq 0$,

является MDS-матрицей, поскольку как ее определитель, так и определители всех ее подматриц размера 2×2 отличны от нуля. При этом в каждой строке и в каждом столбце матрицы стоит как минимум по одному элементу e и α^2 . Перестановки строк и столбцов не изменяют данного свойства.

Кроме того, так как по условию элементы матрицы должны принадлежать множеству $D(\alpha)$, ни столбцы, ни строки матрицы нельзя ни умножать, ни делить на степени элемента α . Следовательно, матрица B не входит в классы матриц, описанные в утверждениях 11 и 12.

Утверждение 13. Пусть $B \in G(D(\alpha), m, m)$, $m = 4, 5$, B — MDS-матрица. Тогда:

- 1) в каждой строке и в каждом столбце матрицы B имеется не более одного элемента α ,
- 2) как число строк, так и число столбцов, в которых элемент α не встречается, не превосходит 1,
- 3) если $m = 5$, то в каждой строке и в каждом столбце матрицы B стоит в точности один элемент α .

Доказательство. По утверждению 10 в любом столбце и в любой строке матрицы может содержаться не более двух элементов α . Рассмотрим элементы матрицы, которые равны α . Перестановкой строк и столбцов приведем матрицу B к виду $B = \begin{pmatrix} B_2 & \cdot & \cdot \\ \cdot & B_1 & \cdot \\ \cdot & \cdot & B_0 \end{pmatrix}$, где B_i , $i = 0, 1, 2$, — квадратные подматрицы матрицы B размеров $m_i \times m_i$, $i = 0, 1, 2$, соответственно. При этом ни вне подматриц B_0 , B_1 и B_2 , ни в подматрице B_0 нет элементов α . В матрице B_1 элементы α стоят только на главной диагонали. Кроме того, матрица B_0 имеет максимальный размер среди всех возможных таких представлений. Каждый элемент α в подматрице B_2 располагается либо в строке, либо в столбце, в котором есть еще один элемент α .

Из утверждения 6 следует, что $m_0 \leq 1$.

Пусть $m_2 \neq 0$. Перестановкой строк и столбцов матрицу B_2 , в свою очередь, также приведем к блочно-диагональному виду так, чтобы, во-первых, элементы α не содержались вне квадратных блоков (подматриц), стоящих на главной диагонали. Во-вторых, чтобы в левом верхнем углу блоков стоял элемент α . И, в-третьих, чтобы в каждом блоке все элементы α (за исключением, может быть, одного) стояли бы рядом либо в строке, либо в столбце. То есть блоки должны иметь вид $\begin{pmatrix} \alpha & \alpha \\ Y & Y \end{pmatrix}$ или $\begin{pmatrix} \alpha & Y \\ \alpha & Y \end{pmatrix}$, или $\begin{pmatrix} \alpha & \alpha \\ Y & \alpha \end{pmatrix}$, или

$$\begin{pmatrix} \alpha & \alpha & Y \\ Y & \alpha & \alpha \\ Y & Y & \alpha \end{pmatrix}, \text{ или } \begin{pmatrix} \alpha & \alpha & Y \\ Y & \alpha & \alpha \\ \alpha & Y & \alpha \end{pmatrix}, \text{ или } \begin{pmatrix} \alpha & \alpha & Y & Y \\ Y & \alpha & \alpha & Y \\ Y & Y & \alpha & \alpha \\ Y & Y & Y & \alpha \end{pmatrix} \text{ и т. д.}$$

При этом символами Y обозначаем произвольные (возможно, совпадающие) элементы из множества $D(\alpha) \setminus \{\alpha\} = \{e, \alpha^2\}$.

Без ограничения общности можем считать, что верхняя левая часть матрицы B имеет вид

$$\begin{pmatrix} \alpha & \alpha & Y & Y \\ Y & X & Y & Y \\ Y & Y & \alpha & X \\ Y & Y & X & X \end{pmatrix},$$

где элемент $b_{33} = \alpha$ (поскольку $m_2 + m_1 = m - m_0 \geq 3$) либо находится все еще в первом блоке (тогда, вообще говоря, можно добавить еще элементов α), либо в начале второго блока подматрицы B_2 , либо это верхний левый элемент матрицы B_1 . Как и в предыдущих утверждениях, символ X обозначает произвольные (возможно, совпадающие) элементы множества $D(\alpha)$.

Пусть $b_{22} \neq \alpha$. Если найдется такое $i \in \{2, 3, 4\}$, что $b_{i1} = b_{i2}$, то $(1, i; 1, 2) \rightarrow Z$. Если же $b_{i1} \neq b_{i2}$ для любого $i \in \{2, 3, 4\}$, то запрет будет находиться на пересечении столбцов с номерами 1 и 2 и строк с соответствующими номерами, поскольку вариантов значений для трех пар всего два. Следовательно, $b_{22} = \alpha$:

$$\begin{pmatrix} \alpha & \alpha & Y & Y \\ Y & \alpha & Y & Y \\ Y & Y & \alpha & X \\ Y & Y & X & X \end{pmatrix}.$$

Пусть $b_{23} \neq \alpha$. Значит, первый блок подматрицы B_2 имеет размер 2×2 . Имеем $b_{13} \neq b_{23}$, иначе $(1, 2; 2, 3) \rightarrow Z$. Кроме того, $b_{13}, b_{23} \in \{e, \alpha^2\}$. Аналогично получаем, что $b_{31} \neq b_{32}$ и $b_{31}, b_{32} \in \{e, \alpha^2\}$. Если $b_{32} = e$, то $(3, i; 2, 3) \rightarrow Z$, где $i = 1, 2$ удовлетворяет условию $b_{i3} = \alpha^2$. Если $b_{32} = \alpha^2$, то $(3, i; 2, 3) \rightarrow Z$, где $i = 1, 2$ удовлетворяет условию $b_{i3} = e$. Следовательно, $b_{23} = \alpha$ (и $b_{43} \neq \alpha$!):

$$\begin{pmatrix} \alpha & \alpha & Y & Y \\ Y & \alpha & \alpha & Y \\ Y & Y & \alpha & X \\ Y & Y & Y & X \end{pmatrix}.$$

Если $b_{21} \neq b_{13}$, то $(1, 2; 1, 3) \rightarrow Z$. Значит, $b_{21} = b_{13}$. Аналогично получаем, что $b_{32} = b_{13}$:

$$\begin{pmatrix} \alpha & \alpha & x & Y \\ x & \alpha & \alpha & Y \\ Y & x & \alpha & X \\ Y & Y & Y & X \end{pmatrix},$$

где x — некоторый фиксированный элемент из $D(\alpha) \setminus \{\alpha\}$. Заметим, что $b_{31} \neq x$ (иначе $(1, 3; 1, 2) \rightarrow Z$).

Если $b_{31} \neq \alpha$, то $b_{31} = y$, где $\{y\} = D(\alpha) \setminus \{\alpha, x\}$. При любых значениях $x, y \in \{e, \alpha^2\}$, $x \neq y$, имеем $(1, 3; 1, 3) \rightarrow Z$. Значит, $b_{31} = \alpha$ (и $b_{34} \neq \alpha$!):

$$\begin{pmatrix} \alpha & \alpha & x & Y \\ x & \alpha & \alpha & Y \\ \alpha & x & \alpha & Y \\ Y & Y & Y & X \end{pmatrix}.$$

Рассмотрим элементы b_{14}, b_{24}, b_{34} . Они выбираются из множества $\{e, \alpha^2\}$ и, значит, среди них есть два совпадающих. Тогда подматрицы на пересечении тех строк, в которых стоят совпадающие элементы, и столбца с номером 4, а также столбца с номером от 1 до 3, в котором два элемента α стоят в тех же строках, что и совпадающие элементы из столбца 4, образуют запрет.

Полученное противоречие означает, что $m_2 = 0$.

Пусть $m = 5$ и $m_0 = 1$. Тогда матрицу B перестановкой строк и столбцов можно привести к виду $\begin{pmatrix} \alpha & Y & Y & Y & Y \\ Y & \alpha & Y & Y & Y \\ Y & Y & \alpha & Y & Y \\ Y & Y & Y & Y & \alpha \\ Y & Y & Y & Y & Y \end{pmatrix}$, и она содержит подматрицу

размера 2×4 , элементы которой могут принимать не более двух значений, что противоречит утверждению 6. Значит, $m_0 = 0$.

Утверждение 13 доказано. $\square$

3. Классификация квадратных $m \times m$ MDS-матриц, $m \geq 4$, над полем $GF(2^t)$, $t \geq 2$, с элементами из множества $D(\alpha) = \{e, \alpha, \alpha^2\}$, $\alpha \neq 0$ и $\alpha \neq e$

Утверждение 14. Пусть B — квадратная MDS-матрица над полем $GF(2^t)$ размера 4×4 , элементы которой принадлежат множеству $D(\alpha) = \{e, \alpha, \alpha^2\}$, $\alpha \neq 0$ и $\alpha \neq e$, и в каждой строке и в каждом столбце имеется ровно один элемент α . Тогда с точностью до перестановки строк и столбцов матрица B имеет вид

$$B = \begin{pmatrix} \alpha & e & e & \alpha^2 \\ e & \alpha & \alpha^2 & e \\ e & \alpha^2 & \alpha & \alpha^2 \\ \alpha^2 & e & \alpha^2 & \alpha \end{pmatrix}. \quad (4)$$

Доказательство. С точностью до перестановки строк и столбцов матрица B имеет вид

$$\begin{pmatrix} \alpha & Y & Y & Y \\ Y & \alpha & Y & Y \\ Y & Y & \alpha & Y \\ Y & Y & Y & \alpha \end{pmatrix},$$

где символы Y обозначают произвольные (возможно, совпадающие) элементы из множества $D(\alpha) \setminus \{\alpha\} = \{e, \alpha^2\}$.

Имеем $b_{ij} = b_{ji}$ при $1 \leq i, j \leq 4$, так как иначе при $i \neq j$ получаем $(i, j; i, j) \rightarrow Z$.

Обозначим через u число элементов матрицы B , равных e . С учетом сказанного $u \in \{0, \dots, 12\}$ и является четным числом.

Из утверждения 6 следует, что $u \neq 0$ и $u \neq 12$.

Пусть $u = 2$ или $u = 10$. Тогда с точностью до перестановки строк и столбцов матрица B имеет вид

$$\begin{pmatrix} \alpha & \beta & \gamma & \gamma \\ \beta & \alpha & \gamma & \gamma \\ \gamma & \gamma & \alpha & \gamma \\ \gamma & \gamma & \gamma & \alpha \end{pmatrix},$$

где $(\beta, \gamma) = (e, \alpha^2)$ при $u = 2$ и $(\beta, \gamma) = (\alpha^2, e)$ при $u = 10$, и содержит запреты, например $(3, 4; 1, 2) \rightarrow Z$. Значит, $u \neq 2$ и $u \neq 10$.

Пусть $u = 4$ или $u = 8$. Тогда с точностью до перестановки строк и столбцов возможны три варианта:

$$\begin{pmatrix} \alpha & \beta & \gamma & \gamma \\ \beta & \alpha & \gamma & \gamma \\ \gamma & \gamma & \alpha & \beta \\ \gamma & \gamma & \beta & \alpha \end{pmatrix}, \quad \begin{pmatrix} \alpha & \beta & \beta & \gamma \\ \beta & \alpha & \gamma & \gamma \\ \beta & \gamma & \alpha & \gamma \\ \gamma & \gamma & \gamma & \alpha \end{pmatrix}, \quad \begin{pmatrix} \alpha & \beta & \gamma & \gamma \\ \beta & \alpha & \beta & \gamma \\ \gamma & \beta & \alpha & \gamma \\ \gamma & \gamma & \gamma & \alpha \end{pmatrix},$$

где

$$(\beta, \gamma) = \begin{cases} (e, \alpha^2) & \text{при } u = 4, \\ (\alpha^2, e) & \text{при } u = 8. \end{cases}$$

Во всех трех вариантах есть запреты, образованные векторами из множества G_3 . Таким образом, $u \neq 4$ и $u \neq 8$, и остается единственный случай $u = 6$.

С точностью до перестановки строк и столбцов можно считать, что матрица B имеет вид $\begin{pmatrix} \alpha & e & Y & Y \\ e & \alpha & Y & Y \\ Y & Y & \alpha & Y \\ Y & Y & Y & \alpha \end{pmatrix}$, а поскольку хотя бы в одной из строк элемент e должен встречаться более одного раза, то можно считать, что матрица B имеет вид $\begin{pmatrix} \alpha & e & e & Y \\ e & \alpha & Y & Y \\ e & Y & \alpha & Y \\ Y & Y & Y & \alpha \end{pmatrix}$.

Если $b_{41} = \alpha$ ($= b_{14}$), то все оставшиеся элементы матрицы, обозначенные через Y , должны быть равны α^2 . Тогда $(1, 2; 3, 4) \rightarrow Z$. Значит, $b_{41} = b_{14} = \alpha^2$:

$$\begin{pmatrix} \alpha & e & e & \alpha^2 \\ e & \alpha & Y & Y \\ e & Y & \alpha & Y \\ \alpha^2 & Y & Y & \alpha \end{pmatrix}.$$

Рассмотрим элементы Y , стоящие под главной диагональю. Один из них должен быть равен e , остальные равны α^2 . Если $b_{32} = e$, то $b_{42} = \alpha^2$. Но тогда $(3, 4; 1, 2) \rightarrow Z$. Значит, $b_{32} = \alpha^2$, и матрица B имеет вид

$$\begin{pmatrix} \alpha & e & e & \alpha^2 \\ e & \alpha & \alpha^2 & Y \\ e & \alpha^2 & \alpha & Y \\ \alpha^2 & Y & Y & \alpha \end{pmatrix}.$$

Далее, возможны 2 варианта:

$$\begin{pmatrix} \alpha & e & e & \alpha^2 \\ e & \alpha & \alpha^2 & e \\ e & \alpha^2 & \alpha & \alpha^2 \\ \alpha^2 & e & \alpha^2 & \alpha \end{pmatrix}, \quad \begin{pmatrix} \alpha & e & e & \alpha^2 \\ e & \alpha & \alpha^2 & \alpha^2 \\ e & \alpha^2 & \alpha & e \\ \alpha^2 & \alpha^2 & e & \alpha \end{pmatrix},$$

которые получаются один из другого перестановкой второй и третьей строк и второго и третьего столбцов.

Утверждение 14 доказано. $\square$

Следствие 5. Матрица B вида (4) является MDS-матрицей тогда и только тогда, когда элемент α не является корнем ни одного из многочленов

$$x^2 + x + e, \quad x^3 + x + e, \quad x^3 + x^2 + e \in GF(2^t)[x].$$

Действительно, поскольку матрица B является MDS-матрицей, определители всех ее квадратных подматриц не равны нулю. Непосредственной проверкой убеждаемся, что если α — корень хотя бы одного из перечисленных трех многочленов, то один из определителей окажется нулевым.

Утверждение 15. Пусть B — квадратная MDS-матрица над полем $GF(2^t)$ размера 5×5 , элементы которой принадлежат множеству $D(\alpha) = \{e, \alpha, \alpha^2\}$, $\alpha \neq 0$ и $\alpha \neq e$. Тогда с точностью до перестановки строк и столбцов матрица B имеет вид

$$B = \begin{pmatrix} \alpha & e & e & \alpha^2 & \alpha^2 \\ e & \alpha & \alpha^2 & e & \alpha^2 \\ e & \alpha^2 & \alpha & \alpha^2 & e \\ \alpha^2 & e & \alpha^2 & \alpha & e \\ \alpha^2 & \alpha^2 & e & e & \alpha \end{pmatrix}. \quad (5)$$

Доказательство. С точностью до перестановки строк столбцов матрица B имеет вид

$$\begin{pmatrix} \alpha & Y & Y & Y & Y \\ Y & \alpha & Y & Y & Y \\ Y & Y & \alpha & Y & Y \\ Y & Y & Y & \alpha & Y \\ Y & Y & Y & Y & \alpha \end{pmatrix},$$

где символы Y обозначают произвольные (возможно, совпадающие) элементы из множества $D(\alpha) \setminus \{\alpha\} = \{e, \alpha^2\}$.

Как и в предыдущем утверждении, имеем $b_{ij} = b_{ji}$ при $1 \leq i, j \leq 5$.

По утверждению 14 подматрицу, стоящую на пересечении первых четырех столбцов и первых четырех строк в матрице B , можно привести перестановкой строк и столбцов к следующему виду:

$$\begin{pmatrix} \alpha & e & e & \alpha^2 & Y \\ e & \alpha & \alpha^2 & e & Y \\ e & \alpha^2 & \alpha & \alpha^2 & Y \\ \alpha^2 & e & \alpha^2 & \alpha & Y \\ Y & Y & Y & Y & \alpha \end{pmatrix}.$$

Рассмотрим вектор-столбцы, расположенные в строках с номерами 2 и 3. По следствию из утверждения 7 последний вектор-столбец может быть только из множества G_0 , и это в точности $\begin{pmatrix} \alpha^2 \\ e \end{pmatrix}$. Тогда

$$B = \begin{pmatrix} \alpha & e & e & \alpha^2 & Y \\ e & \alpha & \alpha^2 & e & \alpha^2 \\ e & \alpha^2 & \alpha & \alpha^2 & e \\ \alpha^2 & e & \alpha^2 & \alpha & Y \\ Y & \alpha^2 & e & Y & \alpha \end{pmatrix},$$

и отсюда однозначно, чтобы не получить запреты, находим $b_{51} = b_{15} = \alpha^2$ и $b_{54} = b_{45} = e$. Утверждение 15 доказано. $\square$

Следствие 6. Матрица B вида (5) является MDS-матрицей тогда и только тогда, когда элемент α не является корнем ни одного из следующих многочленов:

$$x^2 + x + e, \quad x^3 + x + e, \quad x^3 + x^2 + e, \quad x^5 + x^4 + e, \quad x^5 + x + e \in GF(2^t)[x].$$

Действительно, поскольку матрица B является MDS-матрицей, определители всех ее квадратных подматриц не равны нулю. Непосредственной проверкой убеждаемся, что если α — корень хотя бы одного из перечисленных пяти многочленов, то один из определителей окажется нулевым.

Утверждение 16. Пусть B — квадратная MDS-матрица над полем $GF(2^t)$ размера 4×4 , элементы которой принадлежат множеству

$$D(\alpha) = \{e, \alpha, \alpha^2\}, \quad \alpha \neq 0 \quad \text{и} \quad \alpha \neq e,$$

и в которой есть строка, не содержащая α . Тогда перестановкой строк и столбцов, а также транспонированием матрицу B можно привести к виду

$$B = \begin{pmatrix} \alpha & \beta & \beta & \gamma \\ \beta & \alpha & \gamma & \beta \\ \beta & \gamma & \alpha & \gamma \\ \gamma & \gamma & \beta & \beta \end{pmatrix}, \quad (6)$$

где $\{\beta, \gamma\} = \{e, \alpha^2\}$. При этом $(\beta, \gamma) = (e, \alpha^2)$, если число единичных элементов в матрице B больше числа элементов α^2 (случай A), и $(\beta, \gamma) = (\alpha^2, e)$ в противном случае (случай B).

Доказательство. С точностью до перестановки строк и столбцов матрица B имеет вид

$$\begin{pmatrix} \alpha & Y & Y & Y \\ Y & \alpha & Y & Y \\ Y & Y & \alpha & Y \\ Y & Y & Y & Y \end{pmatrix},$$

где символы Y обозначают произвольные (возможно, совпадающие) элементы из множества $D(\alpha) \setminus \{\alpha\} = \{e, \alpha^2\}$.

Отметим, что, как и в предыдущих утверждениях, $b_{ij} = b_{ji}$ при $1 \leq i, j \leq 3$.

Рассмотрим множество векторов $\left\{ \begin{pmatrix} b_{31} \\ b_{41} \end{pmatrix}, \begin{pmatrix} b_{32} \\ b_{42} \end{pmatrix}, \begin{pmatrix} b_{34} \\ b_{44} \end{pmatrix} \right\}$. Это множество совпадает с одним из двух множеств $\left\{ \begin{pmatrix} e \\ \alpha^2 \end{pmatrix}, \begin{pmatrix} \alpha^2 \\ e \end{pmatrix}, \begin{pmatrix} e \\ e \end{pmatrix} \right\}$ или $\left\{ \begin{pmatrix} e \\ \alpha^2 \end{pmatrix}, \begin{pmatrix} \alpha^2 \\ e \end{pmatrix}, \begin{pmatrix} \alpha^2 \\ \alpha^2 \end{pmatrix} \right\}$.

I. Пусть это первое из указанных множеств. Тогда в третьей строке матрицы B элемент e встречается два раза. С точностью до перестановки строк и столбцов можно считать, что $b_{31} = e$.

Тогда матрица имеет вид

$$\begin{pmatrix} \alpha & Y & e & Y \\ Y & \alpha & Y & Y \\ e & Y & \alpha & Y \\ Y & Y & Y & Y \end{pmatrix}.$$

Рассмотрим два случая: 1) $b_{32} = e$ и 2) $b_{32} = \alpha^2$.

1) В этом случае $b_{34} = \alpha^2$ и $b_{44} = e$:

$$\begin{pmatrix} \alpha & Y & e & Y \\ Y & \alpha & e & Y \\ e & e & \alpha & \alpha^2 \\ Y & Y & Y & e \end{pmatrix}.$$

Если $b_{41} = b_{42}$, то $(3, 4; 1, 2) \rightarrow Z$. Значит, $b_{41} \neq b_{42}$. Опять же с точностью до перестановки строк и столбцов можем считать, что матрица B имеет вид

$$\begin{pmatrix} \alpha & Y & e & Y \\ Y & \alpha & e & Y \\ e & e & \alpha & \alpha^2 \\ e & \alpha^2 & Y & e \end{pmatrix}.$$

Аналогично получаем, что $b_{14} \neq b_{24}$ и, значит, $\{b_{14}, b_{24}\} = \{e, \alpha^2\}$. Тогда $b_{43} = \alpha^2$ (иначе имеется запрет). Если $b_{12} = e$, то $(1, 4; 2, 3) \rightarrow Z$. Значит, $b_{12} = b_{21} = \alpha^2$:

$$\begin{pmatrix} \alpha & \alpha^2 & e & Y \\ \alpha^2 & \alpha & e & Y \\ e & e & \alpha & \alpha^2 \\ e & \alpha^2 & \alpha^2 & e \end{pmatrix}.$$

Если $b_{14} = e$, то $(1, 3; 2, 4) \rightarrow Z$. Значит, $b_{14} = \alpha^2$ и, следовательно, $b_{24} = e$:

$$\begin{pmatrix} \alpha & \alpha^2 & e & \alpha^2 \\ \alpha^2 & \alpha & e & e \\ e & e & \alpha & \alpha^2 \\ e & \alpha^2 & \alpha^2 & e \end{pmatrix}.$$

Переставляя в полученной матрице местами строки с номерами 1 и 3, а также столбцы с номерами 1 и 3, получаем требуемый вид (6) в случае А.

2) В этом случае $b_{34} = e$ и $b_{42} = e$:

$$\begin{pmatrix} \alpha & Y & e & Y \\ Y & \alpha & \alpha^2 & Y \\ e & \alpha^2 & \alpha & e \\ Y & e & Y & Y \end{pmatrix}.$$

Возможны два случая: 2.1) $b_{44} = e$ и 2.2) $b_{44} = \alpha^2$.

2.1) Пусть $b_{44} = e$. Если $b_{41} = e$, то $(3, 4; 1, 4) \rightarrow Z$. Значит, $b_{41} = \alpha^2$:

$$\begin{pmatrix} \alpha & Y & e & Y \\ Y & \alpha & \alpha^2 & Y \\ e & \alpha^2 & \alpha & e \\ \alpha^2 & e & Y & e \end{pmatrix}.$$

Пусть $b_{21} = \alpha^2$. Если $b_{24} = \alpha^2$, то $(2, 3; 1, 4) \rightarrow Z$. А если $b_{24} = e$, то $(2, 4; 1, 4) \rightarrow Z$. Полученное противоречие означает, что $b_{21} = b_{12} = e$. Отсюда, в частности, следует, что $b_{24} = \alpha^2$, и тогда $b_{43} = \alpha^2$ и $b_{41} = \alpha^2$ (иначе имеются запреты).

Полученная матрица

$$\begin{pmatrix} \alpha & e & e & \alpha^2 \\ e & \alpha & \alpha^2 & \alpha^2 \\ e & \alpha^2 & \alpha & e \\ \alpha^2 & e & \alpha^2 & e \end{pmatrix}$$

с точностью до транспонирования имеет вид (6) для случая А.

2.2) Пусть $b_{44} = \alpha^2$. Если $b_{41} = \alpha^2$, то $(3, 4; 1, 4) \rightarrow Z$. Значит, $b_{41} = e$:

$$\begin{pmatrix} \alpha & Y & e & Y \\ Y & \alpha & \alpha^2 & Y \\ e & \alpha^2 & \alpha & e \\ e & e & Y & \alpha^2 \end{pmatrix}.$$

Далее, $b_{21} \neq b_{24}$, иначе $(2, 3; 1, 4) \rightarrow Z$. Если $(b_{21}, b_{24}) = (e, \alpha^2)$, то $(2, 4; 1, 4) \rightarrow Z$. Значит, $(b_{21}, b_{24}) = (\alpha^2, e)$:

$$\begin{pmatrix} \alpha & \alpha^2 & e & Y \\ \alpha^2 & \alpha & \alpha^2 & e \\ e & \alpha^2 & \alpha & e \\ e & e & Y & \alpha^2 \end{pmatrix}.$$

Имеем $b_{43} = \alpha^2$, иначе $(2, 4; 1, 3) \rightarrow Z$. Тогда $b_{14} = \alpha^2$. Полученная матрица

$$\begin{pmatrix} \alpha & \alpha^2 & e & \alpha^2 \\ \alpha^2 & \alpha & \alpha^2 & e \\ e & \alpha^2 & \alpha & e \\ e & e & \alpha^2 & \alpha^2 \end{pmatrix}$$

после перестановки столбцов с номерами 1 и 2 и строк с номерами 1 и 2 будет иметь вид (6) для случая В.

II. В утверждении 2 описаны способы преобразования матрицы, которые сохраняют ее свойство оставаться MDS-матрицей. Отметим, что если $B \in G(D(\alpha), m, m)$, то при умножении строк и столбцов этой матрицы на ненулевые элементы можно получить матрицу не из множества $G(D(\alpha), m, m)$.

Если же сделать замену $\alpha = \delta^{-1}$ в матрице $B \in G(D(\alpha), m, m)$, затем умножить каждую ее строку на δ^2 , а потом сделать замену $\delta = \alpha$, то вновь полученная матрица, вообще говоря, будет другой, но опять будет принадлежать множеству $G(D(\alpha), m, m)$. При таком преобразовании матрицы, как нетрудно видеть, элементы e в ней заменяются элементами α^2 , и наоборот. Элементы α остаются без изменений.

Отметим, что при такой замене $e \leftrightarrow \alpha^2$ множества G_i , $i = 0, 1, 2, 3$, переходят сами в себя. Множество $\left\{ \begin{pmatrix} e \\ \alpha^2 \end{pmatrix}, \begin{pmatrix} \alpha^2 \\ e \end{pmatrix}, \begin{pmatrix} \alpha^2 \\ \alpha^2 \end{pmatrix} \right\}$ перейдет в множество $\left\{ \begin{pmatrix} e \\ \alpha^2 \end{pmatrix}, \begin{pmatrix} \alpha^2 \\ e \end{pmatrix}, \begin{pmatrix} e \\ e \end{pmatrix} \right\}$, и мы оказываемся в условиях п. I. Используя полученные результаты и проводя обратную замену $e \leftrightarrow \alpha^2$, получим, что в случае II матрица перестановкой строк и столбцов может быть приведена к виду (6) (случай В), либо опять же перестановкой строк и столбцов и транспонированием приведена к виду (6) (случай В), либо перестановкой строк и столбцов приведена к виду (6) (случай А). Утверждение 16 доказано. $\square$

Следствие 7. Если элемент α не является корнем ни одного из следующих многочленов:

$$x^2 + x + e, \quad x^3 + x + e, \quad x^3 + x^2 + e, \quad x^5 + x^4 + e, \quad x^5 + x + e \in GF(2^t)[x],$$

то любая матрица B вида (6) — MDS-матрица.

Действительно, для любой матрицы B , которая является MDS-матрицей, определители всех ее подматриц не равны нулю. Непосредственной проверкой убеждаемся, что если α — корень хотя бы одного из первых трех перечисленных многочленов, то одна из подматриц размера 2×2 или 3×3 окажется вырожденной как для случая А, так и для случая В. Определитель матрицы B будет равен 0 либо в случае, когда α — корень многочлена $x^5 + x^4 + e$ (случай А), либо в случае, когда α — корень многочлена $x^5 + x + e$ (случай В).

З а м е ч а н и е. В следствиях к утверждениям 14–16 можно считать, что рассматриваемые многочлены — из кольца $GF(2)[x]$.

Пример 2. Над полем $GF(2^2)$ и над полем $GF(2^3)$ нет MDS-матриц размера 4×4 , состоящих только из элементов множества $\{e, \alpha, \alpha^2\}$, $\alpha \neq e$ и $\alpha \neq 0$.

Автор благодарит рецензентов работы за замечания, позволившие существенно улучшить изложение.

Список литературы

- [1] Dehnavi S.M., Mahmoodi R.A., Shamsabad M.R., “Characterization of MDS mappings”, 2015/002. <http://eprint.iacr.org>.
- [2] Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А., *Теория кодов, исправляющих ошибки*, М.: Связь, 1979, 744 с.
- [3] Малышев Ф. М., “Двойственность разностного и линейного методов в криптографии”, *Математические вопросы криптографии*, **5:3** (2014), 35–47.
- [4] Малышев Ф. М., Трифонов Д. И., “Рассеивающие свойства XSLP-шифров”, *Математические вопросы криптографии*, **7:3** (2016), 47–60.
- [5] Daemen J., Rijmen V., “The Rijndael block cipher (AES proposal)” (1999), <http://www.csrc.nist.gov/archiv/aes/rijndael/Rijndael-ammended.pdf>.
- [6] Schnorr C., Vaudenay S., “Black box cryptanalysis of hash networks based on multipermutations”, *Lect. Notes Comput. Sci.*, **950**, 1994, 47–57.
- [7] Vaudenay S., “On the need for multipermutations: cryptanalysis of MD4 and SAFER”, *Lect. Notes Comput. Sci.*, **1008**, 1994, 286–297.
- [8] Biham E., Shamir A., “Differential cryptanalysis of DES-like cryptosystem”, *Lect. Notes Comput. Sci.*, **537**, 1991, 2–21.
- [9] Matsui M., “Linear cryptanalysis method for DES”, *Lect. Notes Comput. Sci.*, **765**, 1993, 386–397.
- [10] Daemen J., *Cipher and hash function design strategies based on linear and differential cryptanalysis*, Ph.D. thesis, Leuven, Belgium: Elektrotechniek Katholieke Univ., 1995.
- [11] Sajadieh M., Dakhilalian M., Mala H., Sepehrdad P., “Recursive diffusion layers for block ciphers and hash functions”, *Lect. Notes Comput. Sci.*, **7549**, 2012, 385–401.
- [12] Guo J., Peyrin T., Poschmann A., “The PHOTON family of lightweight hash functions”, *Lect. Notes Comput. Sci.*, **6841**, 2011, 222–239.
- [13] Guo J., Peyrin T., Poschmann A., Robshaw M., “The LED block cipher”, *Lect. Notes Comput. Sci.*, **6917**, 2011, 326–341.
- [14] Zeng G., He K., Han W., “A trinomial type of σ -LFSR oriented toward software implementation”, *Science in China, Ser. F: Inf. Sci.*, **50** (2007), 359–372.
- [15] Gupta K. C., Ray I. G., “On constructions of involutory MDS matrices”, *Lect. Notes Comput. Sci.*, **7918**, 2013, 43–60.
- [16] Gupta K. C., Ray I. G., “On constructions of MDS matrices from companion matrices for lightweight cryptography”, *Lect. Notes Comput. Sci.*, **8128**, 2013, 29–43.