ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 29 МАТЕМАТИКИ Выпуск 1
2022

Е. С. Кузнецова (Москва, МГТУ им. Н. Э. Баумана). **О представлении обратных матриц к некоторым MDS-матрицам в поле вычетов конечного поля GF(16) по модулю неприводимых многочленов 4 степени.**

УДК 519.719.2 DOI https://doi.org/10.52513/08698325_2022_29_1_??

Резюме: Нахождение MDS-матриц и обратных к ним матриц является интересной задачей современной криптографии. Немаловажно, чтобы вид этих матриц мог быть, по возможности, наиболее просто реализован в реальных условиях. В данной работе были получены обратные матрицы в поле вычетов конечного поля GF(16) по модулю неприводимых многочленов 4 степени, а именно многочленов $(x^4+x+1), (x^4+x^3+1)$ и $(x^4+x^3+x^2+x+1)$, для двух видов MDS-матриц размерности 4×4 и одного размерности 5×5.

Ключевые слова: MDS-матрицы, обратные матрицы, поля вычетов.

Согласно работе [2]: матрица $A_{m\times n}$ является MDS-матрицей, если любая ее квадратная подматрица является невырожденной, т. е. имеющий определитель, отличный от нуля.

Рассмотрим два вида MDS-матриц размерности 4×4 и один размерности 5×5, описанные в [1].

1. Квадратная $m\times m$ MDS-матрица, $m=4$, над полем $\mathbf{GF}(2^t)$, $t>2$, элементы которых принадлежат множеству $D(\alpha)=\{e,\alpha,\alpha^2\}$, где $\alpha\neq 0,e$, в каждой строке и в каждом столбце имеется ровно один элемент α.

С точностью до перестановки строк и столбцов матрица B имеет вид:

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

Обратная матрица имеет вид:

$$B=(\alpha^5+\alpha^3+\alpha+e)^{-1}\begin{pmatrix} f_1(\alpha) & f_2(\alpha) & f_3(\alpha) & f_4(\alpha) \\ f_2(\alpha) & f_1(\alpha) & f_4(\alpha) & f_3(\alpha) \\ f_3(\alpha) & f_4(\alpha) & f_5(\alpha) & f_6(\alpha) \\ f_4(\alpha) & f_3(\alpha) & f_6\alpha) & f_5(\alpha) \end{pmatrix}.$$

Если рассматривать поле $\mathbf{GF}(16)$ как фактор-кольцо по неприводимому многочлену (в данном случае рассматриваются неприводимые многочлены степени 4), то для элемента $(\alpha^5+\alpha^3+\alpha+e)$ можно вычислить обратный и домножить на элементы матрицы B^{-1}, тогда новые элементы примут вид:

1) в случае многочлена (x^4+x+1) :

© Редакция журнала «ОПиПМ», 2022 г.

$$
\begin{aligned}
(\alpha^5+\alpha^3+\alpha+e)^{-1}\cdot f_1(\alpha) &= \alpha^3+\alpha^2+e;\\
(\alpha^5+\alpha^3+\alpha+e)^{-1}\cdot f_2(\alpha) &= \alpha;\\
(\alpha^5+\alpha^3+\alpha+e)^{-1}\cdot f_3(\alpha) &= \alpha^2+\alpha+e;\\
(\alpha^5+\alpha^3+\alpha+e)^{-1}\cdot f_4(\alpha) &= \alpha^2+\alpha;\\
(\alpha^5+\alpha^3+\alpha+e)^{-1}\cdot f_5(\alpha) &= e;\\
(\alpha^5+\alpha^3+\alpha+e)^{-1}\cdot f_6(\alpha) &= \alpha^3+\alpha^2+\alpha+e.
\end{aligned}
$$

2) в случае многочлена (x^4+x^3+1) :

$$
\begin{aligned}
(\alpha^5+\alpha^3+\alpha+e)^{-1}\cdot f_1(\alpha) &= e;\\
(\alpha^5+\alpha^3+\alpha+e)^{-1}\cdot f_2(\alpha) &= \alpha^3;\\
(\alpha^5+\alpha^3+\alpha+e)^{-1}\cdot f_3(\alpha) &= \alpha^3+\alpha;\\
(\alpha^5+\alpha^3+\alpha+e)^{-1}\cdot f_4(\alpha) &= \alpha^3+\alpha+e;\\
(\alpha^5+\alpha^3+\alpha+e)^{-1}\cdot f_5(\alpha) &= \alpha^2;\\
(\alpha^5+\alpha^3+\alpha+e)^{-1}\cdot f_6(\alpha) &= \alpha^3+\alpha^2.
\end{aligned}
$$

3) в случае многочлена $(x^4+x^3+x^2+x+1)$:

$$
\begin{aligned}
(\alpha^5+\alpha^3+\alpha+e)^{-1}\cdot f_1(\alpha) &= \alpha^3+\alpha^2+\alpha+e;\\
(\alpha^5+\alpha^3+\alpha+e)^{-1}\cdot f_2(\alpha) &= \alpha^2;\\
(\alpha^5+\alpha^3+\alpha+e)^{-1}\cdot f_3(\alpha) &= \alpha^3+\alpha+e;\\
(\alpha^5+\alpha^3+\alpha+e)^{-1}\cdot f_4(\alpha) &= \alpha^3+\alpha;\\
(\alpha^5+\alpha^3+\alpha+e)^{-1}\cdot f_5(\alpha) &= \alpha;\\
(\alpha^5+\alpha^3+\alpha+e)^{-1}\cdot f_6(\alpha) &= \alpha^3.
\end{aligned}
$$

2. Квадратная $m\times m$ MDS-матрица, $m=4$, над полем $\mathbf{GF}(2^t)$, $t>2$, элементы которых принадлежат множеству $D(\alpha)=\{e,\alpha,\alpha^2\}$, где $\alpha\neq 0,e$, в которой есть строка, не содержащая элемент α. С точностью до перестановки строк и столбцов матрица B имеет вид:

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

Обратная матрица имеет вид:

$$
B=^{-1}(\alpha^6+\alpha^5+\alpha^2+e)^{-1}\begin{pmatrix}
f_1(\alpha) & f_3(\alpha) & f_4(\alpha) & f_5(\alpha)\\
f_2(\alpha) & f_1(\alpha) & f_2(\alpha) & f_1(\alpha)\\
f_2(\alpha) & f_4(\alpha) & f_6(\alpha) & f_7(\alpha)\\
f_1(\alpha) & f_5(\alpha) & f_7\alpha) & f_8(\alpha)
\end{pmatrix}.
$$

Аналогично матрице пункта 1 получим:

1) в случае многочлена $x^4 + x + 1$) :

$$\begin{aligned}
(\alpha^6 + \alpha^5 + \alpha^2 + e)^{-1} \cdot f_1(\alpha) &= \alpha;\\
(\alpha^6 + \alpha^5 + \alpha^2 + e)^{-1} \cdot f_2(\alpha) &= \alpha^2 + \alpha;\\
(\alpha^6 + \alpha^5 + \alpha^2 + e)^{-1} \cdot f_3(\alpha) &= \alpha^3 + e;\\
(\alpha^6 + \alpha^5 + \alpha^2 + e)^{-1} \cdot f_4(\alpha) &= \alpha^3 + \alpha^2 + \alpha + e;\\
(\alpha^6 + \alpha^5 + \alpha^2 + e)^{-1} \cdot f_5(\alpha) &= \alpha^3;\\
(\alpha^6 + \alpha^5 + \alpha^2 + e)^{-1} \cdot f_6(\alpha) &= \alpha^3 + \alpha + e;\\
(\alpha^6 + \alpha^5 + \alpha^2 + e)^{-1} \cdot f_7(\alpha) &= \alpha^3 + \alpha^2 + \alpha;\\
(\alpha^6 + \alpha^5 + \alpha^2 + e)^{-1} \cdot f_8(\alpha) &= \alpha^3 + \alpha^2.
\end{aligned}$$

2) в случае многочлена $(x^4 + x^3 + 1)$:

$$\begin{aligned}
(\alpha^6 + \alpha^5 + \alpha^2 + e)^{-1} \cdot f_1(\alpha) &= \alpha^3 + \alpha^2 + e;\\
(\alpha^6 + \alpha^5 + \alpha^2 + e)^{-1} \cdot f_2(\alpha) &= \alpha^3 + \alpha^2 + \alpha;\\
(\alpha^6 + \alpha^5 + \alpha^2 + e)^{-1} \cdot f_3(\alpha) &= \alpha^3 + \alpha;\\
(\alpha^6 + \alpha^5 + \alpha^2 + e)^{-1} \cdot f_4(\alpha) &= \alpha^2;\\
(\alpha^6 + \alpha^5 + \alpha^2 + e)^{-1} \cdot f_5(\alpha) &= \alpha^3 + \alpha;\\
(\alpha^6 + \alpha^5 + \alpha^2 + e)^{-1} \cdot f_6(\alpha) &= \alpha^3 + e;\\
(\alpha^6 + \alpha^5 + \alpha^2 + e)^{-1} \cdot f_7(\alpha) &= \alpha^3 + \alpha^2 + \alpha + e;\\
(\alpha^6 + \alpha^5 + \alpha^2 + e)^{-1} \cdot f_8(\alpha) &= \alpha^3.
\end{aligned}$$

3) в случае многочлена $(x^4 + x^3 + x^2 + x + 1)$:

$$\begin{aligned}
(\alpha^6 + \alpha^5 + \alpha^2 + e)^{-1} \cdot f_1(\alpha) &= \alpha^2 + \alpha + e;\\
(\alpha^6 + \alpha^5 + \alpha^2 + e)^{-1} \cdot f_2(\alpha) &= \alpha^3 + e;\\
(\alpha^6 + \alpha^5 + \alpha^2 + e)^{-1} \cdot f_3(\alpha) &= \alpha^3 + e;\\
(\alpha^6 + \alpha^5 + \alpha^2 + e)^{-1} \cdot f_4(\alpha) &= \alpha + e;\\
(\alpha^6 + \alpha^5 + \alpha^2 + e)^{-1} \cdot f_5(\alpha) &= \alpha^2 + e;\\
(\alpha^6 + \alpha^5 + \alpha^2 + e)^{-1} \cdot f_6(\alpha) &= \alpha^3 + \alpha^2 + e;\\
(\alpha^6 + \alpha^5 + \alpha^2 + e)^{-1} \cdot f_7(\alpha) &= \alpha^3 + \alpha^2;\\
(\alpha^6 + \alpha^5 + \alpha^2 + e)^{-1} \cdot f_8(\alpha) &= \alpha^3 + e.
\end{aligned}$$

3. Квадратная m $\times m$ MDS-матрица, $m = 5$ над полем $\mathbf{GF}(2^t)$, $t > 2$, элементы которой принадлежат множеству $D(\alpha) = e, \alpha, \alpha^2$, $\alpha \neq 0$ $\alpha \neq e$, в каждой строке и в каждом столбце имеющая ровно один элемент α

С точностью до перестановки строк и столбцов матрица B имеет вид:

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

Обратная матрица имеет вид:

$$B =^{-1} (\alpha \cdot f(\alpha))^{-1} \begin{pmatrix}
f_1(\alpha) & f_2(\alpha) & f_2(\alpha) & f_3(\alpha) & f_3(\alpha)\\
f_2(\alpha) & f_1(\alpha) & f_3(\alpha) & f_2(\alpha) & f_3(\alpha)\\
f_2(\alpha) & f_3(\alpha) & f_1(\alpha) & f_3(\alpha) & f_2(\alpha)\\
f_3(\alpha) & f_2(\alpha) & f_3\alpha) & f_1(\alpha) & f_2(\alpha)\\
f_3(\alpha) & f_3(\alpha) & f_2\alpha) & f_2(\alpha) & f_1(\alpha)
\end{pmatrix}.$$

Аналогично матрицам пунктов 1 и 2 получим:
1) в случае многочлена $(x^4 + x + 1)$:

$$\begin{aligned}(\alpha \cdot f(\alpha))^{-1} \cdot f_1(\alpha) &= \alpha^3 + e;\\ (\alpha \cdot f(\alpha))^{-1} \cdot f_2(\alpha) &= \alpha^3 + \alpha^2 + e;\\ (\alpha \cdot f(\alpha))^{-1} \cdot f_3(\alpha) &= \alpha^3 + \alpha + e.\end{aligned}$$

2)в случае многочлена $(x^4 + x^3 + 1)$:

$$\begin{aligned}(\alpha \cdot f(\alpha))^{-1} \cdot f_1(\alpha) &= \alpha^3 + \alpha^2;\\ (\alpha \cdot f(\alpha))^{-1} \cdot f_2(\alpha) &= \alpha^3 + \alpha^2 + \alpha + e;\\ (\alpha \cdot f(\alpha))^{-1} \cdot f_3(\alpha) &= e.\end{aligned}$$

3) в случае многочлена $(x^4 + x^3 + x^2 + x + 1)$:

$$\begin{aligned}(\alpha \cdot f(\alpha))^{-1} \cdot f_1(\alpha) &= \alpha^3 + \alpha^2 + \alpha + e;\\ (\alpha \cdot f(\alpha))^{-1} \cdot f_2(\alpha) &= e;\\ (\alpha \cdot f(\alpha))^{-1} \cdot f_3(\alpha) &= \alpha^3.\end{aligned}$$

Полученные результаты планируется использовать для дальнейших исследований наиболее «удобных» видов обратных матриц к приведенным MDS-матрицам. В частности, представляет интерес рассмотрение вышеприведенных элементов матриц в различных базисах для проведения более обоснованного сравнительного анализа.

СПИСОК ЛИТЕРАТУРЫ

1. *Анашкин А. В.* Полное описание одного класса MDS-матриц над конечным полем характеристики 2. — Математические вопросы криптографии, 2017, т. 8, в. 4, с. 5–28. // *Anashkin A. V.* The complete classification of a set of MDS matrices over finite field of characteristic 2. — Mathematical Aspects of Cryptography, Moscow, 2017, v. 8, is. 4, p. 5–28. (In Russian)

   Лось А. Б., *Нестеренко А. Ю.*, *Рожков М. И.* Криптографические методы защиты информации: учебник для академического бакалавриата. 2-е издание. М.: Юрайт, 2016, 473 с.

UDC 519.719.2 DOI https://doi.org/10.52513/08698325_2022_29_1_??

Kuznetsova E. S. (Moscow, Bauman Moscow State Technical University).
On the representation of inverse matrices to some MDS-matrices in the residue field of a finite field $\mathbf{GF}(16)$ modulo irreducible polynomials of degree 4.

Abstract: Finding MDS-matrices and their inverse matrices is an interesting problem in modern cryptography. It is important that the form of these matrices can be, if possible, most simply implemented in real conditions. In this work, inverse matrices were obtained in the residue field of a finite field $\mathbf{GF}(16)$ modulo irreducible polynomials of degree 4, namely, polynomials $(x^4 + x + 1)$, $(x^4 + x^3 + 1)$ and $(x^4 + x^3 + x^2 + x + 1)$, for two types of MDS-matrices of dimension 4×4 and one of dimension 5×5.

Keywords: MDS-matrices, inverse matrices, residue fields.