ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 621.391:519.7+621.391.1:004.7

НЕКОТОРЫЕ СПОСОБЫ ПОСТРОЕНИЯ MDS-МАТРИЦ НАД КОНЕЧНЫМ ПОЛЕМ

О. Кой Пуэнте, Р. А. Де Ла Крус Хименес

ООО «Центр сертификационных исследований», г. Москва, Россия

Предлагаются новые методы построения MDS-матриц с использованием возведения в степень сопровождающих матриц многочленов над конечным полем. Изучается ряд неприводимых многочленов степени $t = 4$ и 6, сопровождающая матрица которых при возведении в соответствующую степень t является MDS-матрицей. Представлен новый метод построения MDS-матриц, ориентированных на низкоресурсную программную и аппаратную реализации.

Ключевые слова: *MDS-матрицы, сопровождающие матрицы многочленов, неприводимые многочлены, линейные регистры сдвига, конечные поля, XOR-сложность.*

DOI 10.17223/20710410/46/1

SOME METHODS FOR CONSTRUCTING MDS-MATRICES OVER FINITE FIELD

O. Coy Puente, R. A. De La Cruz Jiménez

Certification Research Center, Moscow, Russia

E-mail: o.coypuente@gmail.com, djr.antonio537@gmail.com

In this work, we propose new methods for constructing MDS-matrices over finite field by using recursive ones. For some element $\beta \in \mathrm{GF}(2^n)$ and naturals numbers s and k, we study polynomials of the form $x^4 + \beta^k x^3 + \beta x^2 + \beta^k x + 1$ and $x^6 + \beta^s x^5 + \beta^2 x^4 + \beta x^3 + \beta^2 x^2 + \beta^s x + 1$, for which, when $t = 4, 6$, the t-th power of it's companion matrices yields MDS-matrices with irreducible characteristic polynomial. Also, for some finite field elements β and γ, we have found MDS-matrices of the form $\mathcal{M}^4_{(\beta,\gamma)} = (\beta \cdot \mathcal{I}_{4,4} \oplus \gamma \cdot \mathcal{J}_{4,4} \oplus \mathcal{H}_{4,4})^4$, where for appropriate (4×4)-binary matrices $\mathcal{I}_{4,4}, \mathcal{J}_{4,4}, \mathcal{H}_{4,4}$ the resulting linear mappings can be simplified by some special schemes, very attractive for the so-called lightweight cryptography. The multiplication of any vector by the matrices obtained in the paper can be represented by some circuits which improve the cost of this operation implementation in terms of bitwise XOR's.

Keywords: *MDS-matrices, companion matrices, irreducible polynomials, LFSR, finite field, lightweight cryptography, XOR-count.*

Введение

MDS-матрицы часто используются для реализации линейного слоя алгоритмов блочного шифрования и хеш-функций с целью наилучшего рассеивания входных битов при выполнении требований к шифрам, определенных К. Шенноном [1].

Задача нахождения новых методов построения таких матриц, оптимальных с точки зрения реализации, оказывается довольно сложной. В данной работе представлены новые конструкции MDS-матриц на основе сопровождающих матриц многочленов степени $t = 4$ и 6 над полем $\mathrm{GF}(2^8)$. Они реализуются с использованием линейных регистров сдвига на векторах из множества $\mathrm{GF}(2^8)^t$. Эти конструкции ориентированы на использование в низкоресурсной криптографии.

1. Обзор известных результатов

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

1.1. MDS-матрицы

Определение 1 [2]. Показатель рассеивания ρ матрицы $A \in P_{t,t}$ 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 $\mathbf{a} \in P^t$, т. е. количество его ненулевых элементов.

Определение 2 [2, 3]. Матрица $A \in P_{t,t}$ называется MDS-матрицей, если $\rho(A) = t + 1$.

Лемма 1 [4]. Пусть все элементы матрицы A^{-1} ненулевые, где A^{-1} — обратная к матрице $A \in P^*_{t,t}$. Тогда все подматрицы размера $(t-1) \times (t-1)$ матрицы A принадлежат множеству $P^*_{t-1,t-1}$.

Лемма 2 [4]. Матрица A является MDS-матрицей тогда и только тогда, когда все её квадратные подматрицы являются обратимыми матрицами над полем P.

Лемма 3 [4]. Матрица $A \in P_{4,4}$ является MDS-матрицей тогда и только тогда, когда все элементы её обратной матрицы ненулевые и все её подматрицы размера 2×2 являются обратимыми матрицами.

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

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

называется сопровождающей матрицей многочлена $f(x)$.

1.2. XOR-сложность

Способ восприятия и оценки сложности реализации линейного слоя развивался в течение какого-то времени. Было распространено мнение, что конечные элементы

поля с малым весом Хэмминга имеют более низкую сложность аппаратной реализации. В [5] авторы предложили оценивать сложность реализации путём подсчёта количества вентилей XOR, необходимых для умножения элементов поля. Они также показали, что, в отличие от распространённого мнения, элементы с более высоким весом Хэмминга также могут иметь низкую сложность реализации. Используем эту новую характеристику для расчёта сложности реализации линейного слоя.

Определение 4 [5]. XOR-сложность элемента $\alpha \in P$ — это наибольшее количество операций XOR, необходимых для реализации умножения α на произвольный элемент $\beta \in P$.

Пример 1 [5]. Пусть $\mathrm{GF}(2^3) = \mathrm{GF}(2)[x]/(x^3 + x + 1)$ и α — корень многочлена $x^3 + x + 1$. Рассмотрим $\{1, \alpha, \alpha^2\}$ — 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 $b_i \in \mathrm{GF}(2)$, $i = 0, 1, 2$, 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 $\alpha^4 \cdot \beta$ можно отождествить с упорядоченным набором из $\mathrm{GF}(2)^3$ его координат

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

в котором есть четыре операции XOR. Тогда XOR-сложность элемента α^4 равна 4.

Будем обозначать XOR-сложность элемента $\alpha \in \mathrm{GF}(2^n)$ как $\mathsf{XOR}(\alpha)$. Нетрудно проверить, что $\mathsf{XOR}(0) = \mathsf{XOR}(1) = 0$. XOR-сложность строки с номером i матрицы $M = (m_{i,j})$ размера $t \times t$ можно найти по формуле [5]

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

где l_i — количество ненулевых элементов в i-й строке. Тогда можно определить XOR-сложность любой матрицы $M = (m_{i,j}) \in \mathrm{GF}(2^n)_{t,t}$ по формуле

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

Пусть $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{t-1}x^{t-1} + x^t$ и $\{c_1, \ldots, c_s\}$ — множество всех различных ненулевых коэффициентов многочлена $f(x)$. В [6] показано, что для сопровождающей матрицы S_f многочлена $f(x)$ верны следующие равенства:

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

$$\mathsf{XOR}(S_f^k) = k \cdot \mathsf{XOR}(S_f), \quad k \in \mathbb{N}, \tag{2}$$

где l_f — количество ненулевых элементов в последней строке матрицы S_f.

2. MDS-матрицы, построенные с использованием сопровождающих матриц многочленов

В работе [3] авторы осуществляли перебор элементов $a_0, a_1, a_2, \ldots, a_{t-1}$ таким образом, чтобы S_f^t была MDS-матрицей. В данной работе мы применим другой подход.

2.1. Способы построения MDS-матриц размера 4×4

Предложим метод построения MDS-матриц размера 4×4 с характеристическим многочленом

$$f(x) = x^4 + \beta^k x^3 + \beta x^2 + \beta^k x + 1 \in P[x], \tag{3}$$

где $\beta \in \mathrm{GF}(2^n)$; $k \in \mathbb{N}$.

Теорема 1. Пусть $P = \mathrm{GF}(2^n)$, $n \in \mathbb{N}$, $n \geqslant 4$, $f(x) \in P[x]$ — многочлен вида (3). Пусть $\beta \in P \backslash \{0, 1\}$ и $k \in \{2, \ldots, 2^n - 2\}$ подобраны так, что

$$\begin{aligned}
k^2(8k^2+7) &\not\equiv k(14k^2+1) \pmod{\mathrm{ord}(\beta)},\\
\beta &\neq (\beta^k \oplus 1)^2,\\
\beta &\neq (\beta^k \oplus \beta \oplus 1)^2,\\
\beta &\neq (\beta^{k-1} \oplus \beta^{-1} \oplus 1)^2,\\
\beta &\neq \beta^{2k+1} \oplus \beta^2 \oplus 1,\\
\beta &\neq \beta^k(\beta^k \oplus 1),\\
\beta &\neq (\beta^k \oplus \beta \oplus 1)^2 \beta^{-k},\\
\beta &\neq (\beta^k \oplus \beta \oplus 1)\beta^{k+1},\\
\beta^{2k+1} &\neq (\beta^k \oplus 1)^2\\
\beta^{2k+1} &\neq (\beta^{2k} \oplus \beta \oplus 1)^2,\\
\beta^{4k} &\neq (\beta \oplus 1)^2(\beta^{2k} \oplus \beta).
\end{aligned}$$

Тогда S_f^4 — MDS-матрица.

Доказательство. Сопровождающая матрица многочлена $f(x)$ имеет вид

$$S_f = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & \beta^k & \beta & \beta^k \end{pmatrix}.$$

Несложно проверить, что

$$S_f^{-1} = \begin{pmatrix} \beta^k & \beta & \beta^k & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$S_f^4 = \begin{pmatrix} 1 & \beta^k & \beta & \beta^k \\ \beta^k & 1 \oplus \beta^{2k} & \beta^k \oplus \beta^{1+k} & \beta \oplus \beta^{2k} \\ \beta \oplus \beta^{2k} & \beta^k \oplus \beta^{1+k} \oplus \beta^{3k} & 1 \oplus \beta^2 \oplus \beta^{2k} \oplus \beta^{2k+1} & \beta^k \oplus \beta^{3k} \\ \beta^k \oplus \beta^{3k} & \beta \oplus \beta^{4k} & \beta^k \oplus \beta^{3k} \oplus \beta^{1+3k} & 1 \oplus \beta^2 \oplus \beta^{1+2k} \oplus \beta^{4k} \end{pmatrix}.$$

Тогда получим, что матрица S_f^4 и её обратная отличаются только перестановкой строк и столбцов. Из леммы 3 следует, что достаточно показать, что элементы $s'_{i,j}$ матрицы S_f^4 ненулевые для любых $i, j \in \{1, \ldots, 4\}$, так же как и все миноры размера 2×2. Очевидно, что $s'_{1,j} \neq 0$, $j = 1, \ldots, 4$, и $s'_{2,1} \neq 0$. Из условия

$$k^2(8k^2+7) \not\equiv k(14k^2+1) \bmod (\mathrm{ord}(\beta))$$

получим, что $\mathrm{ord}(\beta) \nmid (8k^4 - 14k^3 + 7k^2 - k)$. Так как

$$8k^4 - 14k^3 + 7k^2 - k = k(k-1)(2k-1)(4k-1),$$

имеем $\mathrm{ord}(\beta) \nmid k(k-1)(2k-1)(4k-1)$, тогда $s'_{2,2} \neq 0$, $s'_{2,3} \neq 0$, $s'_{2,4} \neq 0$, $s'_{3,1} \neq 0$, $s'_{3,4} \neq 0$, $s'_{4,1} \neq 0$ и $s'_{4,2} \neq 0$. Для остальных элементов рассмотрим такие утверждения:

1) $s'_{3,2} \neq 0$ и $s'_{3,3} \neq 0$ тогда и только тогда, когда $\beta \neq (\beta^k \oplus 1)^2$;
2) $s'_{4,3} \neq 0$ тогда и только тогда, когда $\beta^{2k+1} \neq (\beta^k \oplus 1)^2$;
3) $s'_{4,4} \neq 0$ тогда и только тогда, когда $\beta^{2k+1} \neq (\beta^{2k} \oplus \beta \oplus 1)^2$.

Докажем, что все миноры размера 2×2 ненулевые. Любая матрица размера 4×4 имеет 36 миноров размера 2×2. Построим семейство (мультимножество) Y, состоящее из всех таких миноров:

$$
\begin{aligned}
Y = \{\ & 1, && \beta^k, && \beta,\\
& \beta \oplus \beta^{2k}, && \beta^k \oplus \beta^{1+k}, && \beta^2 \oplus \beta^{2k},\\
& \beta^k, && 1 \oplus \beta^{2k}, && \beta^k \oplus \beta^{1+k},\\
& \beta^k \oplus \beta^{3k} \oplus \beta^{1+k}, && \beta^{1+2k}, && \beta^k \oplus \beta^{3k} \oplus \beta^{1+k} \oplus \beta^{2+k},\\
& \beta \oplus \beta^{2k}, && \beta^k \oplus \beta^{3k} \oplus \beta^{1+k}, && 1 \oplus \beta^2 \oplus \beta^{2k} \oplus \beta^{1+2k},\\
& \beta^2 \oplus \beta^{2k} \oplus \beta^{4k}, && \beta^k \oplus \beta^{1+k} \oplus \beta^{2+k} \oplus \beta^{1+3k}, && \beta \oplus \beta^3 \oplus \beta^{2k} \oplus \beta^{4k} \oplus \beta^{2+2k},\\
& \beta, && \beta^k \oplus \beta^{1+k}, && \beta^2 \oplus \beta^{2k},\\
& 1 \oplus \beta^2 \oplus \beta^{2k} \oplus \beta^{1+2k}, && \beta^k \oplus \beta^{3k} \oplus \beta^{1+k} \oplus \beta^{2+k}, && \beta \oplus \beta^3,\\
& \beta^k \oplus \beta^{1+k}, && \beta^{1+2k}, && \beta^k \oplus \beta^{3k} \oplus \beta^{1+k} \oplus \beta^{2+k},\\
& \beta^k \oplus \beta^{1+k} \oplus \beta^{2+k} \oplus \beta^{1+3k}, && 1 \oplus \beta^{2k} \oplus \beta^{4k} \oplus \beta^{2+2k}, && \beta^k \oplus \beta^{3k} \oplus \beta^{2+k} \oplus \beta^{3+k},\\
& \beta^2 \oplus \beta^{2k}, && \beta^k \oplus \beta^{3k} \oplus \beta^{1+k} \oplus \beta^{2+k}, && \beta \oplus \beta^3,\\
& \beta \oplus \beta^3 \oplus \beta^{2k} \oplus \beta^{4k} \oplus \beta^{2+2k}, && \beta^k \oplus \beta^{3k} \oplus \beta^{2+k} \oplus \beta^{3+k}, && 1 \oplus \beta^4 \oplus \beta^{4k} \oplus \beta^{2+2k}\}.
\end{aligned}
$$

Удалив совпадающие элементы, построим множество M с элементами семейства Y:

$$
\begin{aligned}
M = \{\ & 1, && \beta^k, && \beta,\\
& \beta \oplus \beta^{2k}, && \beta^k \oplus \beta^{1+k}, && \beta^2 \oplus \beta^{2k},\\
& 1 \oplus \beta^{2k}, && \beta^{1+2k}, && \beta^k \oplus \beta^{3k} \oplus \beta^{1+k} \oplus \beta^{2+k},\\
& 1 \oplus \beta^2 \oplus \beta^{2k} \oplus \beta^{1+2k}, && \beta^2 \oplus \beta^{2k} \oplus \beta^{4k}, && \beta^k \oplus \beta^{1+k} \oplus \beta^{2+k} \oplus \beta^{1+3k},\\
& \beta \oplus \beta^3 \oplus \beta^{2k} \oplus \beta^{4k} \oplus \beta^{2+2k}, && \beta \oplus \beta^3, && 1 \oplus \beta^{2k} \oplus \beta^{4k} \oplus \beta^{2+2k},\\
& \beta^k \oplus \beta^{3k} \oplus \beta^{2+k} \oplus \beta^{3+k}, && 1 \oplus \beta^4 \oplus \beta^{4k} \oplus \beta^{2+2k}\}.
\end{aligned}
$$

Для элементов множества M, совпадающих с элементами матрицы S_f^4, уже показано, что они ненулевые. Доказательство теоремы вытекает из справедливости следующих соотношений:

1) $\beta^2 \oplus \beta^{2k} \neq 0$ тогда и только тогда, когда $\mathrm{ord}(\beta) \nmid (k-1)$;
2) очевидно, что $\beta^{1+2k} \neq 0$ и $\beta \oplus \beta^3 \neq 0$;
3) $\beta^k \oplus \beta^{3k} \oplus \beta^{1+k} \oplus \beta^{2+k} \neq 0$ тогда и только тогда, когда $\beta \neq (\beta^k \oplus \beta \oplus 1)^2$;
4) $1 \oplus \beta^2 \oplus \beta^{2k} \oplus \beta^{1+2k} \neq 0$ тогда и только тогда, когда $\beta \neq (\beta^k \oplus 1)^2$;
5) $\beta^2 \oplus \beta^{2k} \oplus \beta^{4k} \neq 0$ тогда и только тогда, когда $\beta \neq \beta^k(\beta^k \oplus 1)$;
6) $\beta^k \oplus \beta^{1+k} \oplus \beta^{2+k} \oplus \beta^{1+3k} \neq 0$ тогда и только тогда, когда $\beta \neq \beta^{2k+1} \oplus \beta^2 \oplus 1$;
7) $\beta \oplus \beta^3 \oplus \beta^{2k} \oplus \beta^{4k} \oplus \beta^{2+2k} \neq 0$ тогда и только тогда, когда $\beta^{4k} \neq (\beta \oplus 1)^2(\beta^{2k} \oplus \beta)$;
8) $1 \oplus \beta^{2k} \oplus \beta^{4k} \oplus \beta^{2+2k} \neq 0$ тогда и только тогда, когда $\beta \neq (\beta^k \oplus \beta \oplus 1)\beta^{k+1}$;
9) $\beta^k \oplus \beta^{3k} \oplus \beta^{2+k} \oplus \beta^{3+k} \neq 0$ тогда и только тогда, когда $\beta \neq (\beta^{k-1} \oplus \beta^{-1} \oplus 1)^2$;
10) $1 \oplus \beta^4 \oplus \beta^{4k} \oplus \beta^{2+2k} \neq 0$ тогда и только тогда, когда $\beta \neq (\beta^k \oplus \beta \oplus 1)^2\beta^{-k}$.

Теорема доказана. ■

Следствие 1. Пусть $P = \mathrm{GF}(2^n)$, $n \in \mathbb{N}$, $n \geqslant 4$, $f(x) = x^4 + \beta^2 x^3 + \beta x^2 + \beta^2 x + 1$ и элемент $\beta \in P \backslash \{0, 1\}$ такой, что

$$\begin{aligned}\operatorname{ord}(\beta) &\nmid 21,\\ \beta &\neq (\beta\oplus 1)^3,\\ \beta &\neq (\beta\oplus 1)^4,\\ \beta^3 &\neq \beta\oplus 1,\\ \beta^3 &\neq (\beta\oplus 1)^2(\beta^5\oplus 1),\\ \beta^5 &\neq (\beta\oplus 1)^4,\\ \beta^5 &\neq (\beta\oplus 1)(\beta^6\oplus 1).\end{aligned}$$

Тогда S_f^4 — MDS-матрица.

2.2. MDS-матрицы размера 6×6

Предложим метод построения MDS-матриц размера 6×6 над полем $P=\mathrm{GF}(2^8)$ с использованием сопровождающих матриц многочлена

$$f(x)=x^6+\beta^4x^5+\beta^2x^4+\beta x^3+\beta^2x^2+\beta^4x+1\in P[x]. \tag{4}$$

Теорема 2. Пусть $P=\mathrm{GF}(2^8)$, $f(x)\in P[x]$ — многочлен вида (4) и элемент $\beta\in P\backslash\{0,1\}$ подобран так, что

$$\begin{aligned}1 &\neq (\beta\oplus 1)^3(\beta^6(\beta\oplus 1)^2\oplus\beta)^2,\\ (\beta\oplus 1)^2 &\neq \beta^5(\beta^5\oplus 1),\\ (\beta\oplus 1)^{11} &\neq \beta^2(\beta^2\oplus\beta\oplus 1),\\ \beta(\beta\oplus 1)^8 &\neq (\beta^5\oplus 1)(\beta^6\oplus 1),\\ \beta^2(\beta(\beta\oplus 1)^2\oplus 1)^2 &\neq (\beta^5\oplus 1)(\beta^6\oplus\beta^3\oplus 1)^2.\end{aligned}$$

Тогда S_f^6 — MDS-матрица.

Доказательство. Проводится аналогично доказательству теоремы 1. ■

Предложим метод построения MDS-матриц размера 6×6 над полем $P=\mathrm{GF}(2^8)$, представимых в виде шестой степени сопровождающей матрицы многочлена

$$f(x)=x^6+\beta^7x^5+\beta^2x^4+\beta x^3+\beta^2x^2+\beta^7x+1\in P[x]. \tag{5}$$

Теорема 3. Пусть $P=\mathrm{GF}(2^8)$ и $f(x)\in P[x]$ — многочлен вида (5). Тогда если существует элемент $\beta\in P\backslash\{0,1\}$, такой, что

$$(\beta\oplus 1)^{10}(\beta(\beta\oplus 1)^2\oplus 1)^8 \neq (\beta(\beta\oplus 1))^4(\beta^6\oplus 1),$$

то S_f^6 является MDS-матрицей.

Доказательство. Справедливость теоремы проверяется аналогично доказательству теоремы 1. ■

Рассмотрим наиболее интересный случай, когда многочлены вида (3), (4) и (5) являются неприводимыми над соответствующими полями. В этом случае нельзя выделить классы слабых ключей, основанные на наличии у линейного преобразования алгоритма блочного шифрования инвариантных подпространств [7]. В табл. 1 приведены несколько примеров таких многочленов над полем $\mathrm{GF}(2^n)=\mathrm{GF}(2)[x]/g(x)$, где $\deg(g)=n$. Элементы поля записаны в шестнадцатеричном виде. Например, для элемента $\beta\in\mathrm{GF}(2^8)$, такого, что $\beta=x^7+x^5+x^2+1$, используется запись a5.

Таблица 1

Примеры неприводимых многочленов степени t, сопровождающие матрицы которых при возведении в степень t являются MDS-матрицами

n	$g(x)$	t	$f(x)$	S_f^t
4	x^4+x+1	4	$x^4+\mathsf{c}x^3+8x^2+\mathsf{c}x+1$	$\begin{pmatrix} 1 & \mathsf{c} & 8 & \mathsf{c} \\ \mathsf{c} & \mathsf{e} & 6 & 7 \\ 7 & \mathsf{e} & 3 & 4 \\ 4 & 2 & 8 & 6 \end{pmatrix}$
8	$x^8+x^7+x^6+x+1$	4	$x^4+4x^3+2x^2+4x+1$	$\begin{pmatrix} 1 & 4 & 2 & 4 \\ 4 & 11 & \mathsf{c} & 12 \\ 12 & \mathsf{4c} & 35 & 44 \\ 44 & \mathsf{c1} & \mathsf{c4} & \mathsf{e6} \end{pmatrix}$
16	$x^{16}+x^5+x^3+x^2+1$	4	$x^4+112\mathsf{d}x^3+1\mathsf{c}x^2+112\mathsf{d}x+1$	$\begin{pmatrix} 1 & 112\mathsf{d} & 1\mathsf{c} & 112\mathsf{d} \\ 112\mathsf{d} & 297\mathsf{d} & \mathsf{ce0c} & 2960 \\ 2960 & \mathsf{d022} & 518\mathsf{a} & \mathsf{f03} \\ \mathsf{f03} & \mathsf{aa21} & 6406 & \mathsf{d2cb} \end{pmatrix}$
8	$x^8+x^7+x^6+x+1$	6	$x^6+13x^5+\mathsf{f8}x^4+\mathsf{a3}x^3+\mathsf{f8}x^2+13x+1$	$\begin{pmatrix} 1 & 13 & \mathsf{f8} & \mathsf{a3} & \mathsf{f8} & 13 \\ 13 & \mathsf{c7} & 83 & \mathsf{7c} & 33 & \mathsf{3e} \\ \mathsf{3e} & 37 & \mathsf{b3} & \mathsf{bb} & 8 & 17 \\ 17 & \mathsf{b4} & \mathsf{c1} & \mathsf{fe} & \mathsf{4d} & 82 \\ 82 & \mathsf{a5} & \mathsf{1a} & \mathsf{1d} & 50 & \mathsf{ff} \\ \mathsf{ff} & \mathsf{6b} & \mathsf{1b} & 15 & \mathsf{a3} & \mathsf{b9} \end{pmatrix}$
8	$x^8+x^7+x^6+x+1$	6	$x^6+\mathsf{ba}x^5+2\mathsf{a}x^4+\mathsf{b6}x^3+2\mathsf{a}x^2+\mathsf{ba}x+1$	$\begin{pmatrix} 1 & \mathsf{ba} & \mathsf{2a} & \mathsf{b6} & \mathsf{2a} & \mathsf{ba} \\ \mathsf{ba} & \mathsf{7b} & \mathsf{b5} & 64 & \mathsf{b9} & 50 \\ 50 & 9 & \mathsf{8c} & 40 & 93 & \mathsf{a} \\ \mathsf{a} & \mathsf{7e} & \mathsf{ce} & \mathsf{da} & 87 & \mathsf{bd} \\ \mathsf{bd} & \mathsf{d0} & \mathsf{a7} & 4 & 3 & \mathsf{5d} \\ \mathsf{5d} & 80 & 36 & 80 & \mathsf{e2} & \mathsf{3e} \end{pmatrix}$

3. MDS-отображения, построенные с использованием линейных регистров сдвига

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

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

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

В криптосистемах, ориентированных на низкоресурсную реализацию, существенное значение имеет XOR-сложность используемых криптографических примитивов. Нахождение MDS-отображений с небольшим значением данного параметра является актуальной задачей. Предложим несколько способов построения таких отображений.

3.1. Классы MDS-отображений множества $\mathrm{GF}(2^8)^4$

Предложим способ построения MDS-отображений над полем P с помощью многочленов вида $x^t+x+\beta$.

Теорема 4. Пусть $P=\mathrm{GF}(2^8)$, $f(x)=x^4+x+\beta \in P[x]$, $\mathrm{ord}(\beta) \nmid 9$, $(\beta(\beta^3 \oplus 1))^3 \neq 1$. Тогда матрица S_f^{22} является MDS-матрицей над P.

Доказательство. Справедливость теоремы проверяется по аналогии с доказательством теоремы 1. ■

Известно [8], что $f(S_f)=0$. Для многочлена $f(x)=x^4+x+\beta$ из теоремы 4 имеем $S_f^4 = S_f \oplus \beta \cdot E$, где E — единичная матрица размера 4×4. Пусть $E_\beta = \beta \cdot E$. Тогда верны следующие равенства:

$$S_f^{22} = S_f^2(S_f \oplus E_\beta)(S_f \oplus E_\beta)^4 = S_f^2(S_f \oplus E_\beta)(S_f^4 \oplus E_\beta^4) =$$

$$= S_f^2(S_f \oplus E_\beta)(S_f \oplus E_\beta \oplus E_\beta^4) = S_f^2(S_f \oplus E_\beta)(S_f \oplus E_{\beta(\beta^3 \oplus 1)}).$$

Рассмотрим отображение $\psi_\beta : P^4 \longrightarrow P^4$, определённое по правилу

$$\psi_\beta(\mathbf{a}) = \mathbf{a} \cdot E_\beta,$$

для любых $\beta \in P$, $\mathbf{a} \in P^4$. Тогда отображение $L_{f,\beta} : P^4 \longrightarrow P^4$, задаваемое равенством

$$L_{f,\beta}(\mathbf{a}) = \mathbf{a}\,(S_f^{22})^{\mathrm{T}},$$

является MDS-отображением. Пусть $\beta' = \beta(\beta^3 \oplus 1)$. Обозначим через F отображение, соответствующее линейному регистру сдвига с характеристическим многочленом $f(x)$, т. е. $F(\mathbf{a}) = \mathbf{a} \cdot S_f^{\mathrm{T}}$. Действие отображения $L_{f,\beta}$ на векторах из множества P^4 можно представить схемой рис. 1.

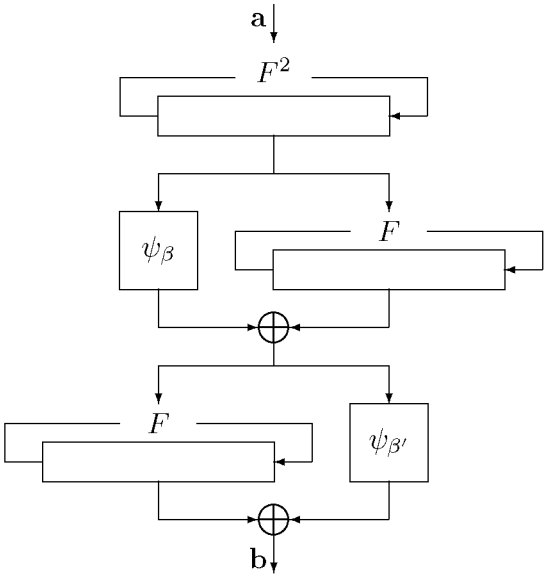

Рис. 1. Действие отображения $L_{f,\beta}$

Рассмотрим теперь MDS-отображения вида

$$\mathbf{a} \mapsto \mathbf{a}(S_f^{\mathrm{T}} \oplus E)^k, \quad \mathbf{a} \in P^t, \tag{6}$$

где S_f — сопровождающая матрица некоторого многочлена $f(x)$ степени t; E — единичная матрица размера $t \times t$. Пусть $f(x) = x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$ — унитарный многочлен степени 4 над полем P. С целью обеспечения эффективной реализации коэффициенты f_i выберем из множества $\{0, 1, \beta, \beta^2\}$. Построим следующие отображения для любого $\mathbf{a} \in P^4$:

Отображение $\mathcal{L}_{f,k}^4$ при $k = 3$
Пусть $\lambda_1(x) = x^4 + \beta^2x^3 + \beta x + \beta^2$. Тогда $\mathcal{L}_{\lambda_1,3}^4(\mathbf{a}) = \mathbf{a}\,(S_{\lambda_1}^{\mathrm{T}} \oplus E)^3$.

Отображение $\mathcal{L}_{f,k}^4$ при $k = 6$
Пусть $\lambda_2(x) = x^4 + \beta x^3 + \beta$. Тогда $\mathcal{L}_{\lambda_2,6}^4(\mathbf{a}) = \mathbf{a}\,(S_{\lambda_2}^{\mathrm{T}} \oplus E)^6$.

Отображение $\mathcal{L}_{f,k}^4$ при $k = 9$
Пусть $\lambda_3(x) = x^4 + x + \beta$. Тогда $\mathcal{L}_{\lambda_3,9}^4(\mathbf{a}) = \mathbf{a}\,(S_{\lambda_3}^{\mathrm{T}} \oplus E)^9$.

Пусть Λ_i — линейное преобразование, соответствующее линейному регистру сдвига с характеристическим многочленом $\lambda_i(x)$ для любого $i = 1, 2, 3$. Тогда действие отображения $\mathcal{L}^4_{\lambda_i,k}$ можно схематично представить рис. 2, где

$$(k_1, k_2) = \begin{cases} (k-i, i), & i = 1, 2, \\ (8, 1), & i = 3. \end{cases}$$

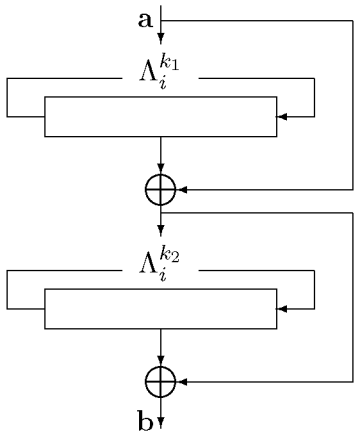

Рис. 2. Действие отображения $\mathcal{L}^4_{\lambda_i,k}$ при $i = 1, 2, 3$

Пусть $P = \mathrm{GF}(2^8)$, $D_1 = \{\beta \in P^* : \mathrm{ord}(\beta) \nmid 9,\ (\beta(\beta^3 \oplus 1))^3 \neq 1\}$. Следующая теорема доказывается аналогично теореме 1.

Теорема 5. Отображения $\mathcal{L}^4_{\lambda_1,3}$, $\mathcal{L}^4_{\lambda_2,6}$ и $\mathcal{L}^4_{\lambda_3,9}$ являются MDS-отображениями для любого $\beta \in D_1$.

3.2. Классы MDS-отображений множества $\mathrm{GF}(2^8)^6$

Пусть $P = \mathrm{GF}(2^8)$. Предложим методы построения MDS-отображений вида (6). Рассмотрим следующие отображения:

Отображение $\mathcal{L}^6_{f,k}$ при $k = 9$
Пусть $\phi_1(x) = x^6 + x^3 + \beta^2 x^2 + \beta$ и $\phi_2(x) = x^6 + \beta^2 x^5 + \beta^2 x^2 + \beta$. Тогда $\mathcal{L}^6_{\phi_1,9}(\mathbf{a}) = \mathbf{a}\,(S^{\mathrm{T}}_{\phi_1} \oplus E)^9$, $\mathcal{L}^6_{\phi_2,9}(\mathbf{a}) = \mathbf{a}\,(S^{\mathrm{T}}_{\phi_2} \oplus E)^9$.

Отображение $\mathcal{L}^6_{f,k}$ при $k = 10$
Пусть $\phi_3(x) = x^6 + \beta^2 x^5 + \beta x^4 + \beta$. Тогда $\mathcal{L}^6_{\phi_3,12}(\mathbf{a}) = \mathbf{a}\,(S^{\mathrm{T}}_{\phi_3} \oplus E)^{10}$.

Пусть Φ_i — линейное преобразование, соответствующее линейному регистру сдвига с характеристическим многочленом $\phi_i(x)$ для любого $i = 1, 2, 3$. Тогда действие отображения $\mathcal{L}^6_{\phi_i,k}$ при соответствующих значениях k можно схематично представить рис. 3, где $k' \equiv k \pmod 8$.

Рассмотрим следующие неприводимые многочлены степени 8 над полем $\mathrm{GF}(2)$:

$$\begin{aligned}
r_1(x) &= x^8 + x^4 + x^3 + x + 1, & r_2(x) &= x^8 + x^5 + x^4 + x^3 + 1, \\
r_3(x) &= x^8 + x^6 + x^5 + x + 1, & r_4(x) &= x^8 + x^6 + x^5 + x^4 + x^2 + x + 1, \\
r_5(x) &= x^8 + x^7 + x^3 + x + 1, & r_6(x) &= x^8 + x^7 + x^4 + x^3 + x^2 + x + 1, \\
r_7(x) &= x^8 + x^7 + x^5 + x + 1, & r_8(x) &= x^8 + x^7 + x^5 + x^3 + 1, \\
r_9(x) &= x^8 + x^7 + x^6 + x + 1, & r_{10}(x) &= x^8 + x^7 + x^6 + x^4 + x^2 + x + 1, \\
r_{11}(x) &= x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + 1, & r_{12}(x) &= x^8 + x^7 + x^6 + x^5 + x^2 + x + 1, \\
r_{13}(x) &= x^8 + x^7 + x^6 + x^5 + x^4 + x + 1, & r_{14}(x) &= x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1.
\end{aligned}$$

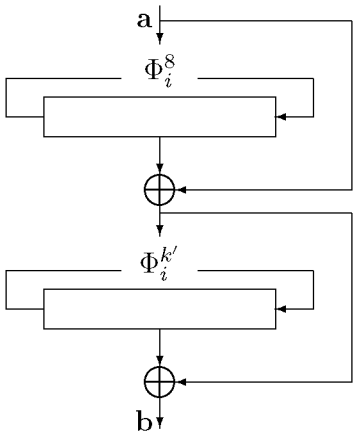

Рис. 3. Действие отображения $\mathcal{L}^6_{\phi_i,k}$ при $i = 1, 2, 3$

Обозначим через $W(r_i)$ множество всех корней многочлена $r_i(x)$ над полем $P = \mathrm{GF}(2^8)$, т. е. $W(r_i) = \{\beta \in P : r_i(\beta) = 0\}$. Следующая теорема доказывается аналогично теореме 1.

Теорема 6. Справедливы утверждения:

1) пусть $\Delta_1 = \{1, 2, 4, 5, 6, 7, 9, 11, 12\} \subset \mathbb{N}$, тогда для любого $\beta \in \bigcup\limits_{i \in \Delta_1} W(r_i)$ отображение $\mathcal{L}^6_{\phi_1,9}$ является MDS-отображением;
2) пусть $\Delta_2 = \{1, 5, 9, 14\} \subset \mathbb{N}$, тогда для любого $\beta \in \bigcup\limits_{i \in \Delta_2} W(r_i)$ отображение $\mathcal{L}^6_{\phi_2,9}$ является MDS-отображением;
3) пусть $\Delta_3 = \{1, 3, 6, 8, 9, 10, 11, 13\} \subset \mathbb{N}$, тогда для любого $\beta \in \bigcup\limits_{i \in \Delta_3} W(r_i)$ отображение $\mathcal{L}^6_{\phi_3,10}$ является MDS-отображением.

4. Построение MDS-матриц вида $(\beta \cdot \mathcal{I}_{4,4} \oplus \gamma \cdot \mathcal{J}_{4,4} \oplus \mathcal{H}_{4,4})^k$

Рассмотрим вопрос о построении MDS-матриц вида $\mathcal{M}^k_{(\beta,\gamma)}$, где

$$\mathcal{M}_{(\beta,\gamma)} = (\beta \cdot \mathcal{I}_{4,4} \oplus \gamma \cdot \mathcal{J}_{4,4} \oplus \mathcal{H}_{4,4});$$

$\mathcal{I}_{4,4}$, $\mathcal{J}_{4,4}$ и $\mathcal{H}_{4,4}$ — произвольные матрицы из $\mathrm{GF}(2)_{4,4}$; элементы β, γ не равны нулю одновременно и принадлежат множеству $\{0, \alpha, \alpha^2\}$, построенному с использованием примитивного элемента $\alpha \in P = \mathrm{GF}(2^8)$. Причиной последнего ограничения является стремление к эффективной реализации при малых значениях k линейного преобразования $\mathcal{M}^k_{(\beta,\gamma)}$. Заметим, что если большинство элементов матрицы $\mathcal{M}_{(\beta,\gamma)}$ равны нулю и среди ненулевых встречаются больше единиц, чем элементов β, γ, то при небольших k матрица $\mathcal{M}^k_{(\beta,\gamma)}$ представляет наибольший интерес.

Был осуществлен поиск на основе случайной генерации матриц $\mathcal{I}_{4,4}$, $\mathcal{J}_{4,4}$ и $\mathcal{H}_{4,4}$ с небольшим количеством единиц; в результате получены матрицы, которые имеют эффективную реализацию (табл. 2). В следующей теореме мы покажем, что эти матрицы являются MDS-матрицами над $P = \mathrm{GF}(2^8)$.

Пусть $p_1(x) = x^2 \oplus x \oplus 1$, $p_2(x) = x^3 \oplus x \oplus 1$, $p_3(x) = x^3 \oplus x^2 \oplus 1$, $p_4(x) = x^4 \oplus x^3 \oplus 1$, $p_5(x) = x^6 \oplus x^3 \oplus 1$, $p_6(x) = x^4 \oplus x^3 \oplus x^2 \oplus x \oplus 1$ — многочлены над полем P.

Теорема 7. Пусть α — примитивный элемент поля $P = \mathrm{GF}(2^8)$. Тогда верны следующие утверждения:

1) если $p_i(\alpha) \neq 0$, $i = 1, 2, 3, 4$, то $\mathcal{M}^4_{(\alpha,0)}$ является MDS-матрицей над P;
2) если $p_i(\alpha) \neq 0$, $i = 1, 2, 3, 4, 5$, то $\mathcal{M}^4_{(\alpha,\alpha^2)}$ является MDS-матрицей над P;

Таблица 2

Несколько матриц вида $(\beta \cdot \mathcal{I}_{4,4} \oplus \gamma \cdot \mathcal{J}_{4,4} \oplus \mathcal{H}_{4,4})^4$

(β,γ)	$\mathcal{M}^4_{(\beta,\gamma)}$	$\mathcal{I}_{4,4}$	$\mathcal{J}_{4,4}$	$\mathcal{H}_{4,4}$	$\mathcal{M}_{(\beta,\gamma)}$
$(\alpha,0)$	$\begin{pmatrix} \alpha & \alpha^2\oplus 1 & \alpha & \alpha \\ \alpha & \alpha^2\oplus\alpha & \alpha^2\oplus 1 & 1 \\ \alpha^2 & \alpha^3 & \alpha & \alpha^3\oplus\alpha \\ \alpha^2\oplus 1 & \alpha^3 & \alpha^2 & \alpha^2\oplus\alpha \end{pmatrix}$	$\begin{pmatrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&1 \\ 0&1&0&0 \end{pmatrix}$	—	$\begin{pmatrix} 0&1&0&0 \\ 0&0&1&1 \\ 0&0&0&1 \\ 1&1&0&0 \end{pmatrix}$	$\begin{pmatrix} 0&1&0&0 \\ 0&0&1&1 \\ 0&0&0&\alpha \\ 1&\alpha&0&0 \end{pmatrix}$
(α^2,α)	$\begin{pmatrix} \alpha^3 & 1 & \alpha^2\oplus\alpha & \alpha^2 \\ \alpha^3\oplus\alpha^2 & \alpha^3\oplus 1 & \alpha^2 & \alpha^2 \\ \alpha & \alpha & \alpha^3\oplus 1 & \alpha^4\oplus\alpha^3 \\ \alpha & \alpha^2\oplus\alpha & 1 & \alpha^3 \end{pmatrix}$	$\begin{pmatrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&1 \\ 0&0&0&0 \end{pmatrix}$	$\begin{pmatrix} 0&0&0&0 \\ 1&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{pmatrix}$	$\begin{pmatrix} 0&0&1&0 \\ 0&0&1&0 \\ 0&1&0&0 \\ 0&1&0&0 \end{pmatrix}$	$\begin{pmatrix} 0&0&1&0 \\ a&0&1&0 \\ 0&1&0&\alpha^2 \\ 0&1&0&0 \end{pmatrix}$
(α,α)	$\begin{pmatrix} \alpha & \alpha^2\oplus 1 & 1 & \alpha^2\oplus\alpha \\ 1 & \alpha^2\oplus\alpha\oplus 1 & \alpha & \alpha^2\oplus\alpha \\ \alpha^2\oplus 1 & \alpha^2\oplus 1 & \alpha^2\oplus\alpha\oplus 1 & \alpha \\ \alpha\oplus 1 & 1 & \alpha\oplus 1 & \alpha \end{pmatrix}$	$\begin{pmatrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&1 \\ 0&0&0&0 \end{pmatrix}$	$\begin{pmatrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&1&0&0 \\ 0&0&0&0 \end{pmatrix}$	$\begin{pmatrix} 0&0&1&0 \\ 1&0&1&0 \\ 0&1&0&0 \\ 0&1&0&0 \end{pmatrix}$	$\begin{pmatrix} 0&0&1&0 \\ 1&0&1&0 \\ 0&\alpha\oplus 1&0&\alpha \\ 0&1&0&0 \end{pmatrix}$

3) если $p_i(\alpha) \neq 0$, $i = 1, 2, 3, 6$, то $\mathcal{M}^4_{(\alpha,\alpha)}$ является MDS-матрицей над P.

Доказательство. Справедливость теоремы показывается аналогично доказательству теоремы 1. ■

Вычисление образа $\mathbf{a} \cdot \mathcal{M}^4_{(\alpha,0)}$ вектора $\mathbf{a} = (a_0, a_1, a_2, a_3)$, как показано на рис. 4, осуществляется в результате четырёхкратной итерации обобщённой сети Фейстеля, которая может быть эффективно реализована, поскольку использует умножение на *фиксированный* элемент поля. Аналогичное представление имеет место для других двух матриц теоремы 7.

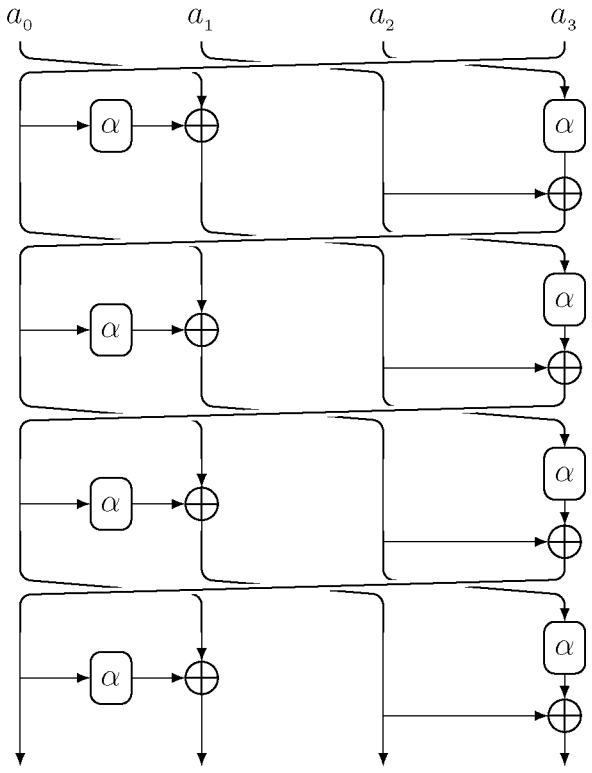

Рис. 4. Действие отображения $\mathbf{a} \cdot \mathcal{M}^4_{(\alpha,0)}$

5. XOR-сложность некоторых MDS-отображений

Пусть $P = \mathrm{GF}(2^8) = \mathrm{GF}(2)[x]/(x^8 + x^7 + x^6 + x + 1)$, α — примитивный элемент поля P и $f(x) = x^t + f_{t-1}x^{t-1} + \ldots + f_1 x + f_0 \in P[x]$, где для любого $i \in \{0, \ldots, t-1\}$ коэффициент $f_i \in \{0, 1, \alpha, \alpha + 1, \alpha^2\}$.

XOR-сложность элементов поля P представлена в табл. 3. Записи соответствуют XOR-сложности элемента, полученного в результате конкатенации соответствующего шестнадцатеричного значения строки и столбца. Например, $\mathsf{XOR}(\mathsf{0x27}) = 28$.

Таблица 3

XOR-сложность элементов поля P

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. 3, приведём следующие рассуждения. Пусть $f(x) = x^4 + x + \beta$. Для сопровождающей матрицы данного многочлена справедливо равенство $\mathsf{XOR}(S_f) = (2-1) \cdot 8 + \mathsf{XOR}(\beta) = \mathsf{XOR}(\beta) + 8$. Найдём $\mathsf{XOR}(L_{f,\beta})$ отображения $L_{f,\beta}$, действие которого представлено на рис. 1. Пусть $\mathbf{z}_{(1)}, \mathbf{z}_{(2)}$ — выход последних двух регистров сдвига данной схемы, $\mathbf{w}_{(1)}, \mathbf{w}_{(2)}$ — выход отображений ψ_β и ψ'_β соответственно. Нетрудно заметить, что $\mathsf{XOR}(L_{f,\beta}) = 4XOR(S_f) + \mathsf{XOR}(\psi_\beta) + \mathsf{XOR}(\mathbf{z}_{(1)} \oplus \oplus \mathbf{w}_{(1)}) + \mathsf{XOR}(\psi'_\beta) + \mathsf{XOR}(\mathbf{z}_{(2)} \oplus \mathbf{w}_{(2)})$. Пусть $\alpha \in P$ такой, что $L_{f,\beta}$ — MDS-отображение и $\mathsf{XOR}(L_{f,\alpha})$ достигает минимального значения среди всех $\beta \in P$, таких, что $L_{f,\beta}$ — MDS-отображение. Тогда при $\beta = \alpha = \mathsf{0x02}$ получим $\mathsf{XOR}(L_{f,\beta}) = 64 + 4\mathsf{XOR}(S_f) + + 4(\mathsf{XOR}(\beta) + \mathsf{XOR}(\beta^4 + \beta)) = 64 + 4 \cdot 11 + 4(3 + 11) = 164$. По формуле (2) получим, что $\mathsf{XOR}(S^{22}) = 22 \cdot 11 = 242$. Из приведённого анализа можно заключить, что лучше использовать для программной и аппаратной реализации схему, представленную на рис. 1, поскольку она менее стоимостная, чем умножение вектора $\mathbf{a} \in P^4$ на матрицу S^{22} из теоремы 4.

Рассмотрим теперь отображения из теорем 5 и 6. По рис. 2 и 3 заметим, что для любого $i \in \{1, 2, 3\}$ при соответствующих значениях k верны равенства $\mathcal{L}^4_{\lambda_i,k}(\mathbf{a}) = = \mathbf{a}((S^{k_1}_{\lambda_i})^{\mathrm{T}} \oplus E)((S^{k_2}_{\lambda_i})^{\mathrm{T}} \oplus E)$ и $\mathcal{L}^6_{\phi_i,k}(\mathbf{a}) = \mathbf{a}((S^8_{\phi_i})^{\mathrm{T}} \oplus E)((S^{k'}_{\phi_i})^{\mathrm{T}} \oplus E)$ соответственно. Для вычисления $(\mathbf{a}(S^{k_1}_{\lambda_i})^{\mathrm{T}} \oplus \mathbf{a}) = \mathbf{z}$ и $(\mathbf{z}(S^{k_2}_{\lambda_i})^{\mathrm{T}} \oplus \mathbf{z}) = \mathbf{b}$ необходимо $2(4 \cdot 8) = = 64$ операции XOR. Аналогичным образом получим, что для реализации операций $(\mathbf{a}(S^8_{\phi_i})^{\mathrm{T}} \oplus \mathbf{a}) = \mathbf{z}$ и $(\mathbf{z}(S^{k'}_{\phi_i})^{\mathrm{T}} \oplus \mathbf{z}) = \mathbf{b}$ необходимо $2(6 \cdot 8) = 96$ операций XOR. Тогда из равенств (1) и (2) следует

$$\mathsf{XOR}(\mathcal{L}^4_{\lambda_i,k}) = k \cdot \mathsf{XOR}(S_{\lambda_i}) + 64, \ \mathsf{XOR}(\mathcal{L}^6_{\phi_i,k}) = k \cdot \mathsf{XOR}(S_{\phi_i}) + 96.$$

Проведём аналогичные рассуждения для матрицы из п. 4. Из табл. 2 можно определить, что количество побитовых операций XOR, необходимых для реализации матриц $\mathcal{M}^4_{(\alpha,0)}$, $\mathcal{M}^4_{(\alpha^2,\alpha)}$ и $\mathcal{M}^4_{(\alpha,\alpha)}$, равно $4 \cdot 22$, $4 \cdot 24$ и $4 \cdot 28$ соответственно.

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

В [3] авторы используют 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 размера 6×6, которые реализованы в семействе хэш-функций PHOTON. Получено, что над полем $\mathrm{GF}(2^n) = \mathrm{GF}(2)[x]/(x^8 + x^4 + x^3 + x + 1)$ матрица $S^6_{g_i}$ является MDS-матрицей, где $i \in \{1, 2\}$. Заметим, что многочлены $g_1(x)$ и $g_2(x)$ имеют вид

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

при некотором $\beta \in \mathrm{GF}(2^n)$. Используя значения из табл. 3 и равенства (1) и (2), получим результаты, представленные в табл. 4 и 5.

Таблица 4

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

MDS-отображения	$S^4_{h_1}$	$S^4_{h_2}$	$S^4_{h_3}$	$L_{f,\alpha}$	$\mathcal{L}^4_{\lambda_1,3}$	$\mathcal{L}^4_{\lambda_2,6}$	$\mathcal{L}^4_{\lambda_3,9}$	$\mathcal{M}^4_{(\alpha,0)}$	$\mathcal{M}^4_{(\alpha^2,\alpha)}$	$\mathcal{M}^4_{(\alpha,\alpha)}$
XOR-сложность	128	144	128	164	136	130	163	88	96	112

Таблица 5

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

MDS-отображения	$S^6_{g'_1}$	$S^6_{g'_2}$	$\mathcal{L}^6_{\phi_1,9}$	$\mathcal{L}^6_{\phi_2,9}$	$\mathcal{L}^6_{\phi_3,10}$
XOR-сложность	366	342	312	312	336

Из табл. 4 и 5 можно сделать следующие выводы:

1) отображения $\mathcal{M}^4_{(\alpha,0)}$, $\mathcal{M}^4_{(\alpha^2,\alpha)}$ и $\mathcal{M}^4_{(\alpha,\alpha)}$ имеют наилучшие значения XOR-сложности среди всех изучаемых отображений, хотя при этом приходится отказаться от использования линейных регистров сдвига для их реализации;
2) аппаратная реализация отображений $\mathcal{L}^6_{\phi_1,9}$, $\mathcal{L}^6_{\phi_2,9}$ и $\mathcal{L}^6_{\phi_3,10}$ менее сложная, чем аппаратная реализация умножения векторов на матрицы ${S_{g'_1}}^6$ и ${S_{g'_2}}^6$.

Заключение

В работе предложены новые методы построения MDS-матриц с помощью рекурсивных процедур. Рассмотренные отображения реализуются с использованием линейных регистров сдвига и обобщённой сети Фейстеля. Они обладают хорошими эксплуатационными характеристиками с точки зрения реализации на вычислительных платформах с ограниченными ресурсами.

ЛИТЕРАТУРА

1. *Shannon C. E.* Communication theory of secrecy systems // Bell System Technical J. 1949. V. 28. No. 4. P. 656–715.

2. *Augot D. and Finiasz M.* Direct construction of recursive MDS diffusion layers using shortened BCH codes // Intern. Workshop on Fast Software Encryption. Springer, 2014. P. 3–17.
3. *Guo J., Peyrin T., and Poschmann A.* The PHOTON family of lightweight hash functions // Ann. Cryptology Conf. Springer, 2011. P. 222–239.
4. *Gupta K. C. and Ray I. G.* On constructions of MDS matrices from companion matrices for lightweight cryptography // Intern. Conf. Availability, Reliability, and Security. Springer, 2013. P. 29–43.
5. *Sarkar S. and Sim S. M.* A deeper understanding of the XOR count distribution in the context of lightweight cryptography // Intern. Conf. Cryptology in Africa. Springer, 2016. P. 167–182.
6. *Toh D., Teo J., Khoo K., and Sim S. M.* Lightweight MDS serial-type matrices with minimal fixed XOR count // Intern. Conf. Cryptology in Africa. Springer, 2018. P. 51–71.
7. *Burov D. A. and Pogorelov B. A.* The influence of linear mapping reducibility on the choice of round constants // Математические вопросы криптографии. 2017. Т. 8. № 2. С. 51–64.
8. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра: 2-е изд., испр. и доп. Санкт-Петербург; Москва; Краснодар: Лань, 2015.

REFERENCES

1. *Shannon C. E.* Communication theory of secrecy systems. Bell System Technical J., 1949, vol. 28, no. 4, pp. 656–715.
2. *Augot D. and Finiasz M.* Direct construction of recursive MDS diffusion layers using shortened BCH codes. Intern. Workshop on Fast Software Encryption, Springer, 2014, pp. 3–17.
3. *Guo J., Peyrin T., and Poschmann A.* The PHOTON family of lightweight hash functions. Ann. Cryptology Conf., Springer, 2011, pp. 222–239.
4. *Gupta K. C. and Ray I. G.* On constructions of MDS matrices from companion matrices for lightweight cryptography. Intern. Conf. Availability, Reliability, and Security, Springer, 2013, pp. 29–43.
5. *Sarkar S. and Sim S. M.* A deeper understanding of the XOR count distribution in the context of lightweight cryptography. Intern. Conf. Cryptology in Africa, Springer, 2016, pp. 167–182.
6. *Toh D., Teo J., Khoo K., and Sim S. M.* Lightweight MDS serial-type matrices with minimal fixed XOR count. Intern. Conf. Cryptology in Africa, Springer, 2018, pp. 51–71.
7. *Burov D. A. and Pogorelov B. A.* The influence of linear mapping reducibility on the choice of round constants. Matematicheskie Voprosy Kriptografii, 2017, vol. 8, no. 2, pp. 51–64.
8. *Glukhov M. M., Elizarov V. P., and Nechaev A. A.* Algebra [Algebra]. St. Petersburg; Moscow; Krasnodar, Lan Publ., 2015. (in Russian)