ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.7

АЛГОРИТМ НАХОЖДЕНИЯ МИНИМАЛЬНОЙ СТЕПЕНИ ПОЛИНОМА НАД КОНЕЧНЫМ ПОЛЕМ ДЛЯ ФУНКЦИИ НАД ВЕКТОРНЫМ ПРОСТРАНСТВОМ В ЗАВИСИМОСТИ ОТ ВЫБОРА НЕПРИВОДИМОГО МНОГОЧЛЕНА

С. А. Белов

Московский государственный университет имени М.В. Ломоносова, г. Москва, Россия

Рассматриваются преобразования над векторным пространством p-ичных векторов длины n, где p — простое число. Каждому такому преобразованию ставится в соответствие полином над конечным полем $\mathrm{GF}(p^n)$. Конечное поле представляется кольцом вычетов по модулю неприводимого многочлена. В общем случае, в зависимости от выбора неприводимого многочлена, преобразованию над векторным пространством соответствуют различные полиномы над конечным полем. Предложен алгоритм поиска минимальной степени среди таких полиномов и неприводимого многочлена, при котором эта степень достигается.

Ключевые слова: *конечное поле, неприводимый многочлен, булевы функции, блочный шифр.*

DOI 10.17223/20710410/43/1

AN ALGORITHM FOR FINDING THE MINIMUM DEGREE OF A POLYNOMIAL OVER A FINITE FIELD FOR A FUNCTION OVER A VECTOR SPACE DEPENDING ON THE CHOICE OF AN IRREDUCIBLE POLYNOMIAL

S. A. Belov

Moscow State University, Moscow, Russia

E-mail: serbel.sci@gmail.com

The transformations of the vector space of p-ary vectors of length n, where p is a prime number, are considered. Each such a transformation is assigned to a polynomial over a finite field $\mathrm{GF}(p^n)$. The finite field is represented by a residue ring modulo an irreducible polynomial. In general, depending on the choice of the irreducible polynomial, different polynomials over the finite field will correspond to the transformation over the vector space. In this paper, we propose an algorithm for finding the minimal degree of such a polynomial and an irreducible polynomial at which this degree is achieved. The algorithm is based on the calculation of expressions for polynomial coefficients through its values. In the process of the algorithm, the elements of finite fields are treated as polynomials. To compute specific irreducible polynomials, the Euclid algorithm computes the greatest common divisor of these expressions and the

polynomial, which is the product of all irreducible polynomials of degree n. To work up to degree d, the algorithm requires storage of $O(p^n n)$ elements from $GF(p)$ and $O(p^n n^2 d^4 w)$ operations of addition and multiplication modulo p where w is the number of elements on which the polynomial is nonzero. Thus, the algorithm is especially effective for functions that have many zero values. The minimal degree polynomials for the S-boxes of block ciphers (GOST 28147-89, ICEBERG, LUFFA, LUCIFER, SERPENT, AES, PRESENT, GOST 34.12-2015) as well as the irreducible polynomials at which this degree is achieved have been computed.

Keywords: *finite field, irreducible polynomial, Boolean functions, block cipher.*

Введение

Пусть задано преобразование $g(x)$ над векторным пространством p-ичных векторов длины n, где p — простое число. Конечное поле $GF(p^n)$ будем рассматривать как кольцо вычетов по неприводимому многочлену $h(\theta)$. При условии, что известно соответствие между p-ичными векторами длины n и элементами конечного поля, каждому преобразованию $g(x)$ можно поставить в соответствие полином $f(x)$ над полем $GF(p^n)$. При различных неприводимых многочленах $h_1(\theta)$ и $h_2(\theta)$ преобразованию $g(x)$ соответствуют, вообще говоря, различные полиномы над конечным полем. В работе рассматривается следующая задача: необходимо найти такой неприводимый многочлен, чтобы в поле, построенном как кольцо вычетов по модулю этого неприводимого многочлена, степень полинома, соответствующего заданному преобразованию над векторным пространством, была наименьшей. Подобная задача рассматривалась в [1] для функций над полями характеристики два. Авторы показали, что полиномы $f_1(x)$ и $f_2(x)$ заданной функции $f(x)$ для пары неприводимых многочленов $R_1(x)$ и $R_2(x)$ связаны соотношением $f_2(x) = L(f_1(L^{-1}(x)))$, где L является обратимым линейным преобразованием рассматриваемого поля. В данной работе предложен иной подход к вычислению минимальной степени многочлена, представляющего функцию над векторным пространством, для различных неприводимых многочленов, который применим для полей произвольной характеристики.

1. Определения и обозначения

Введём определения и обозначения, которые использованы в дальнейшем, а также необходимые утверждения из теории конечных полей [2]:

$GF(q)$ — конечное поле из q элементов. Для конечного поля $GF(q)$ число q имеет вид $q = p^n$, где p — простое число, n — натуральное. Число p называется характеристикой конечного поля. Далее записи $GF(q)$ и $GF(p^n)$ будем считать равнозначными.

$V_n(p)$ — векторное пространство p-ичных векторов длины n с операциями поэлементного сложения векторов по модулю p и умножения вектора на скалярное значение по модулю p. Для пространства $V_1(p)$ будем использовать сокращённую запись $V(p)$.

$F_q[x]$ — множество многочленов переменной x над полем $GF(q)$. Любая функция $f : GF(q) \to GF(q)$ может быть представлена в виде многочлена одной переменной над полем $GF(q)$ степени не более $q - 1$.

Если функция $f : GF(q) \to GF(q)$ представляется полиномом $\sum_{i=0}^{q-1} f_i x^i$, то f_i — коэффициент этого многочлена при степени i.

Весом функции над конечным полем будем называть количество аргументов, на которых она принимает значение, отличное от нуля. НОД двух многочленов $f(x)$ и $g(x)$

будем обозначать $\big(f(x), g(x)\big)$. Носителем булевой функции называется множество наборов, на которых она принимает значение 1.

Множество вычетов по модулю числа p^l-1 относительно операции умножения на p распадается на подмножества, называемые циклотомическими классами по модулю p^l-1 [3]. Циклотомический класс C_s, в котором s — наименьшее число, состоит из чисел

$$C_s = \{s, sp, sp^2, \ldots, sp^{k-1}\},$$

где k — наименьшее натуральное число, для которого $sp^k \equiv s \pmod{p^l-1}$. Старшим представителем циклотомического класса будем называть наибольшее число из этого класса.

Элементы конечного поля $\mathrm{GF}(p^n)$ будем представлять многочленами из $F_p[\theta]$ степени меньше n, сложение и умножение которых осуществляется по модулю заданного неприводимого многочлена. Когда операции над многочленами производятся не по модулю неприводимого многочлена, а по обычным правилам сложения и умножения многочленов в $F_p[\theta]$, будем подчёркивать это, явно записывая переменную θ в скобках. Так, для $a, b \in \mathrm{GF}(q)$ запись $c = ab$ означает умножение двух элементов конечного поля (умножение многочленов по модулю неприводимого многочлена), а запись $a(\theta)b(\theta)$ — обычное умножение многочленов $a(\theta)$ и $b(\theta)$ в кольце $F_p[\theta]$.

Вектору $c = (c_0, c_1, \ldots, c_{n-1})$ из $V_n(p)$ будем ставить в соответствие элемент $\sum\limits_{i=0}^{n-1} c_i\theta^i$ конечного поля $\mathrm{GF}(p^n)$. Для записи элементов конечного поля $\mathrm{GF}(p^n)$ и соответствующих им векторов $V_n(p)$ будем также использовать запись в виде чисел. Вектору $c = (c_0, c_1, \ldots, c_{n-1})$ из $V_n(p)$ (и соответствующему ему элементу поля $\sum\limits_{i=0}^{n-1} c_i\theta^i$) будем ставить в соответствие число $\sum\limits_{i=0}^{n-1} c_i p^i$ из интервала $[0, p^n-1]$. В дальнейшем будем записывать элементы конечного поля в виде многочленов переменной θ или в виде целых чисел, а многочлены, задающие функции над конечными полями, — как многочлены переменной x.

2. Формулы для коэффициентов многочлена над конечным полем

Пусть $\mathrm{GF}(q)$ — конечное поле, $f : \mathrm{GF}(q) \to \mathrm{GF}(q)$. Полином функции f можно записать в канонической форме $f(x) = \sum\limits_{a\in\mathrm{GF}(q)} \delta_a(x)f(a)$, где $\delta_a(x) = \begin{cases} 1, & x = a, \\ 0, & x \neq a. \end{cases}$

В конечном поле верно равенство $\delta_a(x) = 1 - (x-a)^{q-1}$. Подставим выражения для $\delta_a(x)$ и раскроем скобки:

$$\begin{aligned} f(x) &= \sum_{a\in\mathrm{GF}(q)} \delta_a(x)f(a) = \sum_{a\in\mathrm{GF}(q)} (1-(x-a)^{q-1})f(a) = \\ &= \sum_{a\in\mathrm{GF}(q)} (1-(x^{q-1} + ax^{q-2} + \ldots + a^{q-1}))f(a) = \\ &= -\sum_{a\in\mathrm{GF}(q)} (x^{q-1} + ax^{q-2} + \ldots + a^{q-2}x)f(a) + f(0). \end{aligned}$$

Получаем формулу для коэффициентов полинома $f(x)$:

$$f_j = \begin{cases} -\sum\limits_{a\in\mathrm{GF}(q)} a^{q-1-j}f(a), & \text{если } j = 1, 2, \ldots, q-1, \\ f(0), & \text{если } j = 0. \end{cases}$$

Теорема 1 [2]. Произведение $I(q,n,x)$ всех нормированных неприводимых многочленов степени n из кольца $F_q[x]$ задаётся формулой $I(q,n,x) = \prod\limits_{d|n}(x^{q^d} - x)^{\mu(n/d)} =$ $= \prod\limits_{d|n}(x^{q^{n/d}} - x)^{\mu(d)}$, где $\mu(n)$ — функция Мёбиуса:

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1, \\ (-1)^k, & \text{если } n - \text{произведение } k \text{ различных простых чисел}, \\ 0, & \text{если } n \text{ делится на квадрат простого числа}. \end{cases}$$

Утверждение 1. Пусть $h(x)$ — многочлен из кольца $F_p[x]$. Нормированный неприводимый многочлен $g(x)$ степени n, такой, что $g(x)$ делит $h(x)$, существует тогда и только тогда, когда $\big(h(x), I(p,n,x)\big) \neq 1$.

Прежде чем представить алгоритм нахождения минимальной степени полинома, опишем его основную идею. Пусть задана функция $g : V_n(p) \to V_n(p)$. Вопрос, при каком неприводимом многочлена полином f, соответствующий функции g, будет иметь минимальную степень, равносилен вопросу, при каком неприводимом многочлене наибольшее количество коэффициентов $f_{q-1}, f_{q-2}, \ldots, f_1, f_0$, начиная со старших, будет равно нулю. Согласно полученной формуле, $f_j = -\sum\limits_{a \in \mathrm{GF}(q)} a^{q-1-j} f(a)$, $j = 1, 2, \ldots, q-1$. Чтобы установить, при каких неприводимых многочленах $f_j = 0$, достаточно выяснить, какие неприводимые многочлены степени n делят $f_j(\theta) = -\sum\limits_{a \in \mathrm{GF}(q)} a(\theta)^{q-1-j} f(a)(\theta)$. В силу утверждения 1, неприводимый многочлен делит $f_j(\theta)$ тогда и только тогда, когда $\big(f_j(\theta), I(p,n,\theta)\big) \neq 1$ в кольце $F_p[\theta]$. На этом основан алгоритм 1 поиска минимальной степени функции над конечным полем в зависимости от выбора неприводимого многочлена.

Алгоритм 1. Поиск минимальной степени функции

Вход: таблица значений функции g над $V_n(p)$.
Выход: минимальная степень многочлена f над $\mathrm{GF}(p^n)$.

1: $d(\theta) \leftarrow I(p,n,\theta)$
2: **Для** $j = q-1, q-2, \ldots, 1, 0$:
3: **Если** $j > 0$, **то**
4: $f_j(\theta) \leftarrow \sum\limits_{a \in \mathrm{GF}(q)} a(\theta)^{q-1-j} f(a)(\theta)$,
5: **иначе**
6: $f_j(\theta) \leftarrow f(0)(\theta)$.
7: **Если** $f_j(\theta) \neq 0$, **то**
8: $k(\theta) \leftarrow \big(d(\theta), f_j(\theta)\big)$.
9: **Если** $k(\theta) = 1$, **то**
10: **Вернуть** j.
11: $d(\theta) \leftarrow k(\theta)$.
12: **Вернуть** 0.

Отметим, что алгоритм 1 может быть модифицирован таким образом, чтобы дополнительно получать и неприводимый многочлен, при котором достигается минимальная степень. Для этого необходимо на шаге 10, если степень $d(\theta)$ равна n, выдать $d(\theta)$, а если больше n, разложить $d(\theta)$ на множители и выдать любой из сомножителей.

Утверждение 2. Алгоритм 1 всегда возвращает минимальную степень $f(x)$ над $\mathrm{GF}(p^n)$ в зависимости от выбора неприводимого многочлена.

Доказательство. Чтобы показать корректность алгоритма 1, во-первых, отметим, что он всегда завершается и выдаёт ответ. В основном цикле последовательно перебираются коэффициенты полинома $f_j(\theta)$, начиная со старших. Согласно утверждению 1, на шаге 9 $k(\theta)$ является произведением всех неприводимых многочленов степени n, по модулю которых $f_j(\theta) = 0$. Если $k(\theta)$ отличен от 1, то существует неприводимый многочлен степени n, по модулю которого $f_j = 0$. Это означает, что минимальная степень $f(x)$ в зависимости от выбора неприводимого многочлена не более $j-1$. Если $k(\theta)$ равен 1, то неприводимых многочленов степени n, по модулю которых $f_j(\theta) = 0$, не существует, следовательно, минимальная степень $f(x)$ не меньше j. Так как коэффициенты перебираются последовательно, начиная со старших, это означает, что минимальная степень в точности равна j. Особый случай — если функция $f(x)$ тождественно равна 0. Тогда $f_j(\theta)$ будет всё время равен нулю и цикл завершится, пройдя все итерации. В этом случае алгоритм 1 выдаст правильный ответ на шаге 12. ■

Утверждение 3. Сложность проверки с помощью алгоритма 1 того, что степень функции $f(x)$ веса w над полем $\mathrm{GF}(p^n)$ не превосходит d, составляет $\mathrm{O}(p^n n^2 d^4 w)$ операций сложения и умножения по модулю p. При этом необходимо хранить в памяти $\mathrm{O}(p^n n)$ значений из поля $\mathrm{GF}(p)$.

Доказательство. Рассмотрим итерацию с номером j. Обозначим $m = q - 1 - j$. Для вычисления на шаге 4 коэффициента $f_j(\theta)$ требуется вычислить сумму $\sum\limits_{a \in \mathrm{GF}(q)} a(\theta)^{q-1-j} f(a)(\theta)$. Многочлен $a(\theta)$ имеет степень не более $n-1$, для возведения его в степень m требуется не более $\mathrm{O}((mn)^2 \log m)$ операций. Количество слагаемых в сумме равно w, поэтому всего сложность шага 4 составляет $\mathrm{O}(wn^2 m^2 \log m)$ операций.

Если $f_j(\theta) \neq 0$, то происходит вычисление НОД многочленов $f_j(\theta)$ и $d(\theta)$ на шаге 8. Степень многочлена $f_j(\theta)$ не превосходит mn, многочлена $d(\theta) - p^n$. Поэтому сложность вычисления НОД равна $\mathrm{O}(p^n mn)$ [4]. Величина m меняется от 0 до d, суммируя значения сложности по m, имеем

$$\sum_{m=0}^{d} \mathrm{O}(wn^2 m^2 \log m) < \sum_{m=0}^{d} \mathrm{O}(wn^2 m^3) = \mathrm{O}(wn^2 d^4), \quad \sum_{m=0}^{d} \mathrm{O}(p^n nm) = \mathrm{O}(p^n n d^2).$$

Таким образом, полная сложность равна $\mathrm{O}(p^n n^2 d^4 w)$.

В процессе работы алгоритма 1 необходимо хранить многочлены $d(\theta)$ и $k(\theta)$, каждый из которых является многочленом над $\mathrm{GF}(p)$ степени не более p^n, и многочлен $f_j(\theta)$ степени не более $p^n n$. Так как для хранения многочлена степени k над $\mathrm{GF}(p)$ требуется хранить в памяти $\mathrm{O}(k)$ значений из $\mathrm{GF}(p)$, всего для работы алгоритма необходимо хранить $\mathrm{O}(p^n n)$ значений из $\mathrm{GF}(p)$. ■

Замечание 1. Сравним алгоритм 1 с алгоритмом, который последовательно находит остатки от деления на все нормированные неприводимые многочлены степени n. В таком алгоритме шаги 7–11 алгоритма 1 будут заменены на последовательный перебор остатков от деления на все нормированные неприводимые многочлены степени n. Коэффициент $f_j(\theta)$ необходимо вычислить и в том и в другом случае. Степень многочлена $f_j(\theta)$ не превосходит mn. Количество нормированных многочленов степени n над полем $\mathrm{GF}(p)$ имеет порядок p^n/n. При вычислении остатков от деления на все неприво-

димые многочлены полинома $f_j(\theta)$ понадобится $\mathrm{O}\left(\dfrac{p^n}{n} mn \log(mn)\right) = \mathrm{O}(p^n m \log(mn))$ операций сложения и умножения по модулю p. Как показано выше, вычисление НОД на шаге 8 имеет сложность $\mathrm{O}(p^n nm)$ операций. Таким образом, при $m > p^n/n$ сложность вычисления шагов 7–11 алгоритма 1 становится меньше, чем сложность перебора остатков от деления на все неприводимые многочлены степени n.

Пример 1. Пусть $n = 3$, $g(x)$ задаётся таблицей (табл. 1).

Таблица 1

x	0	1	2	3	4	5	6	7
$g(x)$	1	3	4	0	5	6	7	2

Вычислим коэффициенты $f(x)$ согласно алгоритму 1:

$$
\begin{aligned}
&d(\theta) = I(2,3,\theta) = \theta^6 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + \theta + 1;\\
&f_7(\theta) = 1 + (\theta+1) + \theta^2 + 0 + (\theta^2+1) + (\theta^2+\theta) + (\theta^2+\theta+1) + \theta = 0;\\
&f_6(\theta) = 0\cdot 1 + 1\cdot(\theta+1) + \theta\cdot\theta^2 + (\theta+1)\cdot 0 + \theta^2(\theta^2+1) + (\theta^2+1)(\theta^2+\theta) +\\
&\qquad + (\theta^2+\theta)(\theta^2+\theta+1) + (\theta^2+\theta+1)\theta = \theta^4 + \theta^3 + \theta^2 + 1;\\
&k(\theta) = \big(d(\theta), f_6(\theta)\big) = \theta^3 + \theta + 1;\\
&d(\theta) = k(\theta) = \theta^3 + \theta + 1;\\
&f_5(\theta) = 0^2\cdot 1 + 1^2(\theta+1) + \theta^2\cdot\theta^2 + (\theta+1)^2\cdot 0 + (\theta^2)^2(\theta^2+1) + (\theta^2+1)^2(\theta^2+\theta) +\\
&\qquad + (\theta^2+\theta)^2(\theta^2+\theta+1) + (\theta^2+\theta+1)^2\theta = \theta^6 + \theta^5 + \theta + 1;\\
&k(\theta) = \big(d(\theta), f_5(\theta)\big) = 1.
\end{aligned}
$$

В результате минимальная степень $f(x)$ равна 5 и достигается в поле $F_2/(\theta^3+\theta+1)$. При этом в полях с другими неприводимыми многочленами степень функции равна 6.

Пусть функция $g : V_n(p) \to V_n(p)$ задана в виде вектора функций $(g^{(0)}, \ldots, g^{(n-1)})$, где $g^{(i)} : V_n(p) \to V(p)$, при этом для полинома $f(x)$ над $\mathrm{GF}(p^n)$ выполнено $f(x) = \sum\limits_{i=0}^{n-1} \theta^i f^{(i)}(x)$, где полином $f^{(i)}$ соответствует функции $g^{(i)}$, $f^{(i)} : \mathrm{GF}(p^n) \to \mathrm{GF}(p)$. В этом случае шаги 3–6 алгоритма 1 могут быть модифицированы (алгоритм 2).

Алгоритм 2. Модификация алгоритма 1

Вход: таблицы значений функций $g^{(0)}, \ldots, g^{(n-1)}$.
Выход: минимальная степень многочлена f над $\mathrm{GF}(p^n)$.

1: $d(\theta) \leftarrow I(p,n,\theta)$.
2: **Для** $j = q-1, q-2, \ldots, 1, 0$:
3: **Если** $j > 0$, **то**
4: $\quad f_j(\theta) \leftarrow \sum\limits_{i=0}^{n-1} \theta^i \left(\sum\limits_{a \in \mathrm{GF}(q)} a(\theta)^{q-j-1} f^{(i)}(a)(\theta) \right)$,
5: **иначе**
6: $\quad f_j(\theta) \leftarrow \sum\limits_{i=0}^{n-1} \theta^i f^{(i)}(0)(\theta)$.
7: **Если** $f_j(\theta) \neq 0$, **то**
8: $\quad k(\theta) \leftarrow \big(d(\theta), f_j(\theta)\big)$.
9: $\quad$ **Если** $k(\theta) = 1$, **то**
10: $\quad\quad$ **Вернуть** j.
11: $\quad d(\theta) \leftarrow k(\theta)$.
12: **Вернуть** 0.

Отличие алгоритма 2 от алгоритма 1 состоит в способе вычисления коэффициентов $f_j(\theta)$ на шагах 3–6. Все утверждения, относящиеся к алгоритму 1, верны и для алгоритма 2.

3. Случай полей характеристики два

Рассмотрим случай полей характеристики два. Если $q = 2^n$, а $f(x)$ — булева функция от n переменных, то

$$f_j = \begin{cases} \sum\limits_{a \in \mathrm{GF}(2^n), f(a)=1} a^{2^n-1-j}, & \text{если } j = 1, 2, \ldots, 2^n - 1, \\ f(0), & \text{если } j = 0. \end{cases}$$

Следствие 1. Вне зависимости от выбора неприводимого многочлена, полином булевой функции нечётного веса имеет степень $2^n - 1$, чётного веса — не более $2^n - 2$.

Следствие 2. При $n > 2$ полином булевой функции чётного веса имеет степень меньше $2^n - 3$ тогда и только тогда, когда $\sum\limits_{a \in \mathrm{GF}(2^n), f(a)=1} a = 0$, то есть если покоординатная сумма векторов, составляющих носитель булевой функции, равна нулю. Коэффициенты f_{2^n-2} и f_{2^n-3} не зависят от выбора неприводимого многочлена.

Доказательство. Следует из формулы для f_{2^n-2} и того, что $f_{2^n-3} = (f_{2^n-2})^2$. ■

Для булевых функций алгоритм 1 может быть оптимизирован. Так как известно, что для функции $f(x)$ над $\mathrm{GF}(2^n)$ выполнено $f_{2j \bmod (2^n-1)} = f_j^2$, $j = 1, \ldots, 2^n - 2$ [5], то если коэффициент $f_j(\theta)$ равен нулю, то все коэффициенты с номерами из того же циклотомического класса по модулю 2 также равны нулю. Поэтому в цикле достаточно рассмотреть только те j, для которых $2^n - 1 - j$ являются старшими представителями циклотомических классов.

4. Криптографические применения

Описанные алгоритмы могут быть применены в задачах криптоанализа. Они позволяют выбрать представление конечного поля таким образом, чтобы степень исследуемых отображений была как можно меньше. Поиск такого представления уменьшает сложность применения методов криптоанализа, связанных с алгебраическими характеристиками исследуемого отображения, например интерполяционного криптоанализа [6]. В качестве криптографических отображений были проанализированы S-блоки шифров ГОСТ 28147-89 [7, 8], ICEBERG [9], LUFFA [10], LUCIFER [11], SERPENT [12], AES [13], PRESENT [14], ГОСТ Р 34.12-2015 (Кузнечик) [15]. Результаты приведены в табл. 2. Для каждого S-блока вычислена минимальная степень в зависимости от выбора неприводимого многочлена. Указан многочлен, при котором достигается минимальная степень.

Таблица 2

S-box	Степени S-блоков		Многочлен
	Макс.	Мин.	
GOST-A-ParamSet S1 – S8	14	14	Любой
GOST-B-ParamSet S1	14	14	Любой
GOST-B-ParamSet S2	14	13	$\theta^4 + \theta + 1$
GOST-B-ParamSet S3 – S5	14	14	Любой
GOST-B-ParamSet S6 – S8	14	13	$\theta^4 + \theta^3 + 1$
GOST-C-ParamSet S1 – S4	14	14	Любой
GOST-C-ParamSet S5	14	13	$\theta^4 + \theta + 1$
GOST-C-ParamSet S6	14	14	Любой

Окончание табл. 2

S-box	Степени S-блоков		Многочлен
	Макс.	Мин.	
GOST-C-ParamSet S7	14	13	$\theta^4+\theta+1$
GOST-C-ParamSet S8	14	14	Любой
GOST-D-ParamSet S1	14	13	$\theta^4+\theta^3+\theta^2+\theta+1$
GOST-D-ParamSet S2 – S8	14	14	Любой
GOST-T-ParamSet S1	14	13	$\theta^4+\theta^3+1$
GOST-T-ParamSet S2	14	14	Любой
GOST-T-ParamSet S3	14	13	$\theta^4+\theta^3+\theta^2+\theta+1$
GOST-T-ParamSet S4	14	13	$\theta^4+\theta^3+\theta^2+\theta+1$
GOST-T-ParamSet S5	14	13	$\theta^4+\theta^3+1$
GOST-T-ParamSet S6 – S8	14	14	Любой
GOST-Z-ParamSet S1 – S8	14	14	Любой
ICEBERG S0, S1	13	13	Любой
LUFFA	14	14	Любой
Lucifer S0, S1	14	14	Любой
Present	14	14	Любой
Serpent S0	14	14	Любой
Serpent S1	14	13	$\theta^4+\theta^3+1$
Serpent S2 – S7	14	14	Любой
Кузнечик	254	253	$\theta^8+\theta^4+\theta^3+\theta+1$
AES	254	254	Любой

Продемонстрируем вид конкретных полиномов на примере S-блока шифра Кузнечик, который задаётся массивом значений $f=(f(0),f(1),\ldots,f(255))$ [15]:

$f=(252,238,221,17,207,110,49,22,251,196,250,218,35,197,4,77,233,119,240,219,147,46,153,186,23,54,241,187,20,205,95,193,249,24,101,90,226,92,239,33,129,28,60,66,139,1,142,79,5,132,2,174,227,106,143,160,6,11,237,152,127,212,211,31,235,52,44,81,234,200,72,171,242,42,104,162,253,58,206,204,181,112,14,86,8,12,118,18,191,114,19,71,156,183,93,135,21,161,150,41,16,123,154,199,243,145,120,111,157,158,178,177,50,117,25,61,255,53,138,126,109,84,198,128,195,189,13,87,223,245,36,169,62,168,67,201,215,121,214,246,124,34,185,3,224,15,236,222,122,148,176,188,220,232,40,80,78,51,10,74,167,151,96,115,30,0,98,68,26,184,56,130,100,159,38,65,173,69,70,146,39,94,85,47,140,163,165,125,105,213,149,59,7,88,179,64,134,172,29,247,48,55,107,228,136,217,231,137,225,27,131,73,76,63,248,254,141,83,170,144,202,216,133,97,32,113,103,164,45,43,9,91,203,155,37,208,190,229,108,82,89,166,116,210,230,244,180,192,209,102,175,194,57,75,99,182).$

В поле с неприводимым многочленом $\theta^8+\theta^4+\theta^3+\theta+1$ степень многочлена этой функции равна 253, и многочлен имеет следующий вид (коэффициенты полинома, являющиеся элементами конечного поля, записаны в числовом виде):

$$f(x)=158x^{253}+217x^{252}+132x^{251}+45x^{250}+90x^{249}+221x^{248}+175x^{246}+207x^{245}+8x^{244}+18x^{243}+$$
$$+89x^{242}+56x^{241}+162x^{240}+158x^{239}+125x^{238}+139x^{237}+137x^{236}+227x^{235}+204x^{234}+207x^{233}+$$
$$+41x^{232}+x^{231}+41x^{230}+83x^{229}+4x^{228}+59x^{227}+135x^{226}+163x^{225}+51x^{224}+103x^{223}+154x^{222}+$$
$$+249x^{221}+145x^{220}+214x^{219}+63x^{218}+198x^{217}+107x^{216}+42x^{215}+37x^{214}+194x^{212}+210x^{211}+$$
$$+107x^{210}+100x^{209}+202x^{208}+227x^{207}+81x^{206}+95x^{205}+77x^{204}+174x^{203}+114x^{202}+128x^{201}+$$
$$+233x^{200}+37x^{199}+161x^{198}+234x^{197}+15x^{196}+58x^{195}+7x^{194}+102x^{193}+70x^{192}+55x^{191}+119x^{190}+$$
$$+149x^{189}+77x^{188}+35x^{187}+32x^{186}+143x^{185}+30x^{184}+59x^{183}+56x^{182}+10x^{181}+217x^{180}+32x^{179}+$$
$$+66x^{178}+126x^{177}+224x^{176}+199x^{175}+93x^{174}+91x^{173}+134x^{172}+185x^{171}+88x^{170}+156x^{169}+$$
$$+233x^{168}+187x^{167}+6x^{166}+148x^{165}+231x^{164}+66x^{163}+51x^{162}+176x^{161}+84x^{160}+172x^{159}+$$
$$+98x^{158}+73x^{157}+132x^{156}+185x^{155}+113x^{154}+243x^{153}+111x^{152}+183x^{151}+38x^{150}+129x^{149}+$$

$$+88x^{148}+83x^{147}+236x^{146}+176x^{145}+235x^{144}+253x^{143}+158x^{142}+35x^{141}+186x^{140}+44x^{139}+$$
$$+197x^{138}+223x^{137}+133x^{136}+127x^{135}+201x^{134}+217x^{133}+70x^{132}+102x^{131}+121x^{130}+100x^{129}+$$
$$+242x^{128}+27x^{127}+84x^{126}+111x^{125}+138x^{124}+77x^{123}+123x^{122}+68x^{121}+10x^{120}+58x^{119}+$$
$$+140x^{118}+142x^{117}+16x^{116}+41x^{115}+230x^{114}+227x^{113}+96x^{112}+72x^{111}+159x^{110}+37x^{109}+$$
$$+14x^{108}+201x^{107}+5x^{106}+202x^{105}+17x^{104}+175x^{103}+105x^{102}+137x^{101}+204x^{100}+37x^{99}+64x^{98}+$$
$$+195x^{97}+185x^{96}+73x^{95}+193x^{94}+211x^{93}+28x^{92}+245x^{91}+76x^{90}+113x^{89}+238x^{88}+206x^{87}+$$
$$+88x^{86}+70x^{85}+62x^{84}+25x^{83}+167x^{82}+225x^{81}+233x^{80}+32x^{79}+241x^{78}+194x^{77}+36x^{76}+$$
$$+208x^{75}+165x^{74}+252x^{73}+171x^{72}+118x^{71}+234x^{70}+249x^{69}+23x^{68}+234x^{67}+7x^{66}+243x^{65}+$$
$$+66x^{64}+140x^{63}+142x^{62}+x^{61}+217x^{60}+87x^{59}+105x^{58}+174x^{57}+116x^{56}+228x^{55}+238x^{54}+$$
$$+236x^{53}+241x^{52}+18x^{51}+81x^{50}+221x^{49}+138x^{48}+178x^{47}+28x^{46}+160x^{45}+161x^{44}+129x^{43}+$$
$$+56x^{42}+130x^{41}+81x^{40}+207x^{39}+185x^{38}+57x^{37}+207x^{36}+22x^{35}+99x^{34}+242x^{33}+205x^{32}+$$
$$+168x^{31}+x^{30}+36x^{29}+94x^{28}+96x^{27}+158x^{26}+251x^{25}+32x^{24}+217x^{23}+58x^{22}+86x^{21}+207x^{20}+$$
$$+132x^{19}+171x^{18}+113x^{17}+199x^{16}+36x^{15}+246x^{14}+89x^{13}+5x^{12}+111x^{11}+200x^{10}+139x^{9}+$$
$$+172x^{8}+109x^{7}+163x^{6}+176x^{5}+170x^{4}+187x^{3}+110x^{2}+140x+252.$$

В полях с другими неприводимыми многочленами эта функция имеет степень 254, например для поля с неприводимым многочленом $\theta^8+\theta^4+\theta^3+\theta^2+1$ многочлен имеет следующий вид:

$$f(x)=184x^{254}+200x^{253}+124x^{252}+119x^{251}+76x^{250}+195x^{249}+74x^{248}+216x^{247}+134x^{246}+$$
$$+206x^{245}+24x^{244}+62x^{243}+174x^{242}+214x^{241}+158x^{240}+111x^{239}+228x^{238}+199x^{237}+234x^{236}+$$
$$+84x^{235}+164x^{234}+109x^{233}+174x^{232}+134x^{231}+47x^{230}+85x^{229}+182x^{228}+146x^{227}+93x^{226}+$$
$$+189x^{225}+254x^{224}+194x^{223}+205x^{222}+2x^{221}+240x^{220}+7x^{219}+166x^{218}+231x^{217}+134x^{216}+$$
$$+251x^{215}+78x^{214}+146x^{213}+204x^{212}+29x^{211}+79x^{210}+91x^{209}+111x^{208}+229x^{207}+225x^{206}+$$
$$+45x^{205}+106x^{204}+121x^{203}+36x^{202}+134x^{201}+205x^{200}+65x^{199}+210x^{198}+127x^{197}+38x^{196}+$$
$$+166x^{195}+133x^{194}+22x^{193}+253x^{192}+229x^{191}+204x^{190}+148x^{189}+224x^{188}+112x^{187}+134x^{186}+$$
$$+253x^{185}+96x^{184}+240x^{183}+195x^{182}+165x^{181}+119x^{180}+167x^{179}+7x^{178}+150x^{177}+143x^{176}+$$
$$+213x^{175}+165x^{174}+113x^{173}+107x^{172}+134x^{171}+127x^{170}+213x^{169}+109x^{168}+238x^{167}+176x^{166}+$$
$$+165x^{165}+17x^{164}+105x^{163}+78x^{162}+36x^{161}+231x^{160}+81x^{159}+34x^{158}+126x^{157}+134x^{156}+$$
$$+178x^{155}+70x^{154}+24x^{153}+138x^{152}+71x^{151}+84x^{150}+115x^{149}+145x^{148}+144x^{147}+240x^{146}+$$
$$+63x^{145}+34x^{144}+15x^{143}+224x^{142}+134x^{141}+16x^{140}+249x^{139}+255x^{138}+207x^{137}+242x^{136}+$$
$$+108x^{135}+163x^{134}+182x^{133}+132x^{132}+136x^{131}+36x^{130}+155x^{129}+189x^{128}+74x^{127}+134x^{126}+$$
$$+99x^{125}+5x^{124}+251x^{123}+118x^{122}+77x^{121}+76x^{120}+38x^{119}+15x^{118}+141x^{117}+233x^{116}+$$
$$+100x^{115}+136x^{114}+155x^{113}+17x^{112}+134x^{111}+249x^{110}+147x^{109}+74x^{108}+81x^{107}+103x^{106}+$$
$$+116x^{105}+59x^{104}+74x^{103}+174x^{102}+80x^{101}+57x^{100}+172x^{99}+153x^{98}+40x^{97}+134x^{96}+93x^{95}+$$
$$+199x^{94}+147x^{93}+169x^{92}+164x^{91}+133x^{90}+60x^{89}+46x^{88}+30x^{87}+200x^{86}+7x^{85}+75x^{84}+$$
$$+185x^{83}+87x^{82}+134x^{81}+6x^{80}+196x^{79}+243x^{78}+199x^{77}+104x^{76}+87x^{75}+84x^{74}+3x^{73}+89x^{72}+$$
$$+172x^{71}+50x^{70}+150x^{69}+56x^{68}+200x^{67}+134x^{66}+165x^{65}+238x^{64}+52x^{63}+214x^{62}+193x^{61}+$$
$$+134x^{60}+166x^{59}+191x^{58}+155x^{57}+137x^{56}+110x^{55}+227x^{54}+184x^{53}+21x^{52}+134x^{51}+21x^{50}+$$
$$+227x^{49}+234x^{48}+175x^{47}+24x^{46}+111x^{45}+23x^{44}+12x^{43}+11x^{42}+180x^{41}+183x^{40}+131x^{39}+$$
$$+69x^{38}+93x^{37}+134x^{36}+81x^{35}+42x^{34}+149x^{33}+2x^{32}+146x^{31}+157x^{30}+135x^{29}+82x^{28}+74x^{27}+$$
$$+46x^{26}+227x^{25}+145x^{24}+9x^{23}+176x^{22}+134x^{21}+114x^{20}+53x^{19}+67x^{18}+36x^{17}+156x^{16}+$$
$$+190x^{15}+103x^{14}+110x^{13}+101x^{12}+89x^{11}+162x^{10}+245x^{9}+37x^{8}+85x^{7}+134x^{6}+67x^{5}+239x^{4}+$$
$$+174x^{3}+8x^{2}+65x+252.$$

Заключение

В работе предложен алгоритм, находящий минимальную степень полинома $f(x)$ в зависимости от выбора неприводимого многочлена для отображения $g : V_n(p) \to V_n(p)$, и вариация алгоритма для случая, когда отображение задано вектором функций $g_i : V_n(p) \to V(p)$, $i = 0, \ldots, n-1$. Отдельно рассмотрен случай полей характеристики два, в котором выражения для коэффициентов полинома, соответствующего отображению над векторным пространством, имеют особенно простой вид. Для нелинейных блоков замены некоторых блочных шифров вычислены минимальные степени полиномов над конечным полем и указаны неприводимые многочлены, при которых эти минимальные степени достигаются.

ЛИТЕРАТУРА

1. *Youssef A. M. and Gong G.* On the interpolation attacks on block ciphers // Intern. Workshop on Fast Software Encryption. Berlin, Heidelberg, 2000. P. 109–120.
2. *Lidl R. and Niederreiter H.* Finite Fields. Cambridge: Cambridge University Press, 1997. V. 20.
3. *McWilliams F. J. and Sloane N. J. A.* The Theory of Error-Correcting Codes. N.Y.: Elsevier, 1977.
4. *Sorenson J.* An analysis of Lehmer's Euclidean GCD algorithm // Proc. Intern. Symp. on Symbolic and Algebraic Computation. Montreal, Canada, 1995. P. 257–397.
5. *Carlet C.* Boolean functions for cryptography and error correcting codes // Y. Crama and P. Hammer (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge: Cambridge University Press, 2010. P. 257–397.
6. *Jakobsen T. and Knudsen L. R.* The interpolation attack on block ciphers // Intern. Workshop on Fast Software Encryption. Springer, 1997. P. 28–40.
7. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. М.: Издательство стандартов, 1989.
8. *Popov V., Kurepkin I., and Leontiev S.* RFC 4357: Additional Cryptographic Algorithms for Use with GOST 28147–89, GOST R 34.10–94, GOST R 34.10–2001 and GOST R 34.11–94 Algorithms. M.: IETF, 2006.
9. *Standaert F. X., Piret G., Rouvroy G., et al.* ICEBERG: An involutional cipher efficient for block encryption in reconfigurable hardware // Intern. Workshop on Fast Software Encryption. Berlin, Heidelberg, 2004. P. 279–298.
10. *De Canniere C., Sato H., and Watanabe D.* Hash Function Luffa: Specification. Submission to NIST SHA-3 Competition. 2008. `http://www.hitachi.com/rd/yrl/crypto/luffa`.
11. *Sorkin A.* Lucifer, a cryptographic algorithm // Cryptologia. 1984. V. 8. No. 1. P. 22–42.
12. *Biham E., Anderson R., and Knudsen L.* Serpent: A new block cipher proposal // Intern. Workshop on Fast Software Encryption. Berlin, Heidelberg, 1998. P. 222–238.
13. *Daemen J. and Rijmen V.* The Design of Rijndael. AES — the Advanced Encryption Standard. Berlin, Heidelberg: Springer Science & Business Media, 2013.
14. *Bogdanov A., Knudsen L. R., Leander G., et al.* PRESENT: An ultra-lightweight block cipher // Intern. Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg, 2007. P. 450—466.
15. Информационная технология. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2015.

REFERENCES

1. *Youssef A. M. and Gong G.* On the interpolation attacks on block ciphers. Intern. Workshop on Fast Software Encryption. Berlin, Heidelberg, 2000, pp. 109–120.
2. *Lidl R. and Niederreiter H.* Finite Fields. Cambridge, Cambridge University Press, 1997, vol. 20.
3. *McWilliams F. J. and Sloane N. J. A.* The Theory of Error-Correcting Codes. N.Y., Elsevier, 1977.
4. *Sorenson J.* An analysis of Lehmer's Euclidean GCD algorithm. Proc. Intern. Symp. on Symbolic and Algebraic Computation, Montreal, Canada, 1995, pp. 257–397.
5. *Carlet C.* Boolean functions for cryptography and error correcting codes. Y. Crama and P. Hammer (eds.). Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge, Cambridge University Press, 2010, pp. 257–397.
6. *Jakobsen T. and Knudsen L. R.* The interpolation attack on block ciphers. Intern. Workshop on Fast Software Encryption, Springer, 1997, pp. 28–40.
7. GOST 28147–89. Sistemy obrabotki informatsii. Zashchita kriptograficheskaya. Algoritm kriptograficheskogo preobrazovaniya [GOST 28147–89. Information Processing Systems. Cryptographic Protection. Algorithm of Cryptographic Transformation.] Moscow, Standards Publ., 1989. (in Russian)
8. *Popov V., Kurepkin I., and Leontiev S.* RFC 4357: Additional Cryptographic Algorithms for Use with GOST 28147–89, GOST R 34.10–94, GOST R 34.10–2001 and GOST R 34.11–94 Algorithms. Moscow, IETF, 2006.
9. *Standaert F. X., Piret G., Rouvroy G., et al.* ICEBERG: An involutional cipher efficient for block encryption in reconfigurable hardware. Intern. Workshop on Fast Software Encryption, Berlin, Heidelberg, 2004, pp. 279—298.
10. *De Canniere C., Sato H., and Watanabe D.* Hash Function Luffa: Specification. Submission to NIST SHA-3 Competition, 2008. `http://www.hitachi.com/rd/yrl/crypto/luffa`.
11. *Sorkin A.* Lucifer, a cryptographic algorithm. Cryptologia, 1984, vol. 8, no. 1, pp. 22–42.
12. *Biham E., Anderson R., and Knudsen L.* Serpent: A new block cipher proposal. Intern. Workshop on Fast Software Encryption, Berlin, Heidelberg, 1998, pp. 222–238.
13. *Daemen J. and Rijmen V.* The Design of Rijndael. AES — the Advanced Encryption Standard. Berlin, Heidelberg, Springer Science & Business Media, 2013.
14. *Bogdanov A., Knudsen L. R., Leander G., et al.*PRESENT: An ultra-lightweight block cipher. Intern. Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg, 2007, pp. 450–466.
15. Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Blochnyye shifry.[Information Technology. Cryptographic Protection of Information. Block Ciphers.] Moscow, Standartinform Publ., 2015. (in Russian)