

ВЗАИМНО ОДНОЗНАЧНЫЕ БИНОМИАЛЬНЫЕ ФУНКЦИИ НАД КОНЕЧНЫМИ ПОЛЯМИ^{*)}

А. В. Милосердов

Новосибирский гос. университет,
ул. Пирогова, 1, 630090 Новосибирск, Россия

E-mail: amiloserdov6@gmail.com

Аннотация. Рассматриваются биномиальные функции над конечным полем порядка 2^n . Найдено необходимое условие взаимной однозначности биномиальной функции. Доказано, что в случае простого числа $2^n - 1$ взаимно однозначных биномиальных функций не существует. Построены взаимно однозначные биномиальные функции в случае составного n , и найдены взаимно однозначные биномиальные функции для $n \leq 8$. Табл. 2, библиогр. 30.

Ключевые слова: векторная булева функция, биномиальная функция, взаимная однозначность, APN-функция.

Введение

В криптографии в основе симметричных шифров лежат, как правило, S-блоки. Как известно, S-блоки — это векторные булевы функции. В большинстве случаев S-блоки являются перестановками, т. е. взаимно однозначными функциями. Для программной и аппаратной реализации S-блока с помощью вычислительных систем хорошо подходит его полиномиальное представление. Например, полиномиальное представление S-блоков используется в AES — современном стандарте симметричного шифрования США [18].

Задача исследования взаимно однозначных векторных булевых функций возникает на пути поиска функций с полезными криптографическими свойствами, такими как высокая алгебраическая иммунность, низкая

^{*)}Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проекты № 18-31-00374, 18-07-01394), Министерства образования и науки (задание № 1.12875.2018/12.1 и программа 5-100) и Программы фундаментальных научных исследований СО РАН № I.5.1. (проект № 0314-2016-0017).

дифференциальная равномерность, высокая нелинейность и др. [2, 27]. Особый интерес представляют дифференциально 2-равномерные функции, которые называются *APN-функциями*. Такие функции оптимальны для использования в криптографических приложениях в качестве S-блоков с точки зрения дифференциальных характеристик. Активно изучаются методы построения взаимно однозначных APN-функций [1, 4]. До сих пор не решены многие вопросы, связанные со взаимно однозначными функциями, в частности, не найдено общего для всех функций алгоритма проверки взаимной однозначности за время, меньшее, чем время полного просмотра всех значений функции. Один из алгоритмов «медленной» проверки взаимной однозначности рассмотрен в [29]. Также в [29] приведены методы построения взаимно однозначных функций в полиномиальном представлении.

Векторная булева функция может быть отождествлена с функцией над полем \mathbb{F}_{2^n} и единственным образом представлена в виде

$$F(y) = a_0 + \sum_{k=1}^{2^n-1} a_k y^k, \quad \text{где } a_i, y \in \mathbb{F}_{2^n}.$$

Такой вид называется *полиномиальным представлением векторной булевой функции*. Программная и аппаратная реализация функции будет проще, если в её полиномиальном представлении будет небольшое число мономов.

Мономиальные функции обладают самой простой полиномиальной формой, а именно $F(y) = a + by^k$, где $a, b \in \mathbb{F}_{2^n}$ и $1 \leq k \leq 2^n - 1$, и хорошо исследованы. Известны шесть классов мономиальных APN-функций [9] и пять классов бент-функций, которые являются линейными проекциями мономиальных векторных булевых функций [5, 13] (подробнее см. п. 3.1). Также интересно отметить, что функция обращения $F(y) = y^{2^n-2}$ используется в симметричном шифре AES [17].

Биномиальные функции имеют вид $F(y) = ay^i + by^j + c$, где $a, b, c \in \mathbb{F}_{2^n}$, $a \neq 0$, $b \neq 0$, $1 \leq i, j \leq 2^n - 1$, $i \neq j$. В отличие от мономиальных функций, о биномиальных функциях известно немного. Одним из известных примеров является серия бент-функций в виде линейной проекции биномиальных функций $f(x) = \text{tr}(ax^{d_1} + bx^{d_2})$. Известны примеры этих функций с так называемыми показателями Нихо вида $d = 2^i \bmod (2^{n/2} - 1)$. Без ограничения общности можно считать [20], что первый показатель равен $d_1 = \frac{1}{2}(2^{\frac{n}{2}} - 1) + 1$. Если $d_2 = \lambda(2^{\frac{n}{2}} - 1) + 1$, где λ равно $\frac{1}{6}$, $\frac{1}{4}$ или 3, то существуют элементы $a, b \in \mathbb{F}_{2^n}$ такие, что $f(x) = \text{tr}(ax^{d_1} + bx^{d_2})$ является бент-функцией [21]. Вопрос построения

таких функций рассмотрен в [30]. Также в [8] изучены некоторые классы биномиальных APN-функций. В [6] представлен обзор существующих классов биномиальных и мономиальных APN-функций. В [7, 23] приведены оценки на степени мономов для взаимно однозначных функций $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ вида $F(x) = ax^{d_1} + x^{d_2}$, $a \in \mathbb{F}_{2^n}$ (одна из таких оценок приводится в п. 2.3).

В данной статье исследуются взаимно однозначные биномиальные функции над конечными полями. Доказано необходимое условие взаимной однозначности биномиальной функции, и найдены условия существования таких функций при различных ограничениях на число переменных. В статье приводятся найденные биномиальные функции при числе переменных, меньшем либо равном 8, среди которых дифференциально 4-равномерные и функции с максимальной алгебраической иммунностью.

В разд. 1 даны все необходимые определения и утверждения. В разд. 2 рассмотрены векторные булевы функции в полиномиальном представлении, приведён краткий обзор известных результатов для мономиальных (п. 2.1), биномиальных (п. 2.2) функций и функций общего вида (п. 2.4), получено необходимое условие свойства взаимной однозначности функции $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ вида $F(x) = \alpha^k x^i + x^j$ (п. 2.3), а также доказано существование взаимно однозначных функций данного вида в случае составного числа переменных n (п. 2.4). В разд. 3 найдены все взаимно однозначные векторные биномиальные функции при числе переменных, меньшем либо равном 8, и исследованы криптографические свойства найденных функций (п. 3.2). В разд. 4 приведён обзор полученных в работе результатов.

1. Основные понятия и утверждения

1.1. Векторные булевы функции. Функция $f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$, где $\mathbb{F}_2 = \{0, 1\}$, называется *булевой функцией* от n переменных. Функция $F: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ называется *векторной булевой функцией* от n переменных.

Пусть $a, b \in \mathbb{F}_2^n$. Будем обозначать через $a \oplus b$ покомпонентное сложение по модулю два двух булевых векторов a и b .

Любая функция $F: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ представима единственным образом в *алгебраической нормальной форме* (АНФ), или в виде полинома Жегалкина

$$F(x_1, x_2, \dots, x_n) = a \oplus \bigoplus_{k=1}^n \bigoplus_{1 \leq i_1 < \dots < i_k \leq n} a_{i_1, \dots, i_k} x_{i_1} x_{i_2} \dots x_{i_k},$$

где $a, a_{i_1}, \dots, a_{i_k} \in \mathbb{F}_2^m$. Алгебраической степенью (или степенью) векторной булевой функции F называется число переменных в самом длинном слагаемом её АНФ, при котором стоит ненулевой коэффициент.

Функция $F: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ называется *взаимно однозначной*, если для любых двух различных элементов $y_1, y_2 \in \mathbb{F}_2^n$ выполнено $F(y_1) \neq F(y_2)$. Функция $F: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ называется *линейной*, если для любых элементов $y_1, y_2 \in \mathbb{F}_2^n$ верно $F(y_1 + y_2) = F(y_1) + F(y_2)$.

Функция $F: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ называется *дифференциально δ -равномерной*, если уравнение $F(y) \oplus F(y \oplus a) = b$ для любых $a, b \in \mathbb{F}_2^m$, $a \neq 0$, имеет не более δ решений. В случае $\delta = 2$ такая функция называется *APN-функцией* [25].

Алгебраической иммунностью $\text{AI}(f)$ булевой функции $f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ называется минимальное число d такое, что существует булева функция g степени d , не тождественно равная нулю, для которой выполняется равенство $fg = 0$ или $(f \oplus 1)g = 0$. Известно [27], что $\text{AI}(f) \leq \lceil \frac{n}{2} \rceil$. Компонентной алгебраической иммунностью $\text{AI}_{\text{comp}}(F)$ векторной булевой функции $F: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ называется минимальная алгебраическая иммунность компонентных функций $\langle b, F \rangle$, ($b \in \mathbb{F}_2^m$, $b \neq 0$), т. е.

$$\text{AI}_{\text{comp}}(F) = \min \{ \text{AI}(\langle b, F \rangle) \mid b \in \mathbb{F}_2^m, b \neq 0 \},$$

где $\langle b, F \rangle = b_1 f_1 \oplus \dots \oplus b_m f_m$.

Обозначим через $\gcd(a, b)$ *наибольший общий делитель* двух целых чисел a и b .

1.2. Векторная булева функция как функция над конечным полем. Пусть \mathbb{F}_{2^n} — конечное поле из 2^n элементов. Элемент $\alpha \in \mathbb{F}_{2^n}$ называется *примитивным*, если все элементы $\alpha, \alpha^2, \dots, \alpha^{2^n-1}$ попарно различны. Пусть x — переменная, некоторый формальный символ, неизвестная величина, не принадлежащая множеству \mathbb{F}_2 . *Многочленом* (или *полиномом*) степени k над \mathbb{F}_2 называется формальное выражение

$$a(x) = a_k x^k + a_{k-1} x^{k-1} + \dots + a_1 x + a_0,$$

где $a_i \in \mathbb{F}_2$. Такие многочлены можно складывать, при этом их суммой будет многочлен, полученный путём сложения по модулю два коэффициентов при соответствующих степенях.

Многочлен f называется *неприводимым* над полем \mathbb{F}_2 , если его невозможно разложить на множители степеней больше 0 и меньше степени многочлена f с коэффициентами из \mathbb{F}_2 . Пусть задан неприводимый многочлен $g(x)$ степени n . Каждому вектору из \mathbb{F}_2^n можно сопоставить

элемент из \mathbb{F}_{2^n} . Будем сопоставлять вектору $(b_{n-1}, b_{n-2}, \dots, b_0)$ полином $b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \dots + b_0$. Определим операции сложения и умножения следующим образом:

$$\begin{aligned} b + b' &= d, \quad \text{где } d(x) = b(x) + b'(x), \\ c \cdot c' &= d, \quad \text{где } d(x) = c(x) \cdot c'(x) \bmod g(x). \end{aligned}$$

Относительно этих операций \mathbb{F}_2^n является полем. Таким образом, поле \mathbb{F}_{2^n} состоит из всевозможных многочленов от переменной x степени меньше n с коэффициентами из поля \mathbb{F}_2 .

Пусть задано натуральное число a и $(a_k, a_{k-1}, \dots, a_0)$ — его двоичное представление. Будем говорить, что число a принадлежит \mathbb{F}_{2^n} , если k меньше, чем n . Число единиц в двоичном представлении числа a будем называть его *весом* и обозначать через $wt(a)$.

Любая функция $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ представляется *единственным* образом [16] в виде полинома степени не более чем $2^n - 1$:

$$F(y) = a_0 + \sum_{k=1}^{2^n-1} a_k y^k, \quad \text{где } a_i \in \mathbb{F}_{2^n}.$$

Данное представление называется *полиномиальным представлением* векторной булевой функции. Функция $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ называется *мономиальной*, если она имеет вид $F(y) = ay^i + b$, где $a, b \in \mathbb{F}_{2^n}$, $a \neq 0$, $1 \leq i \leq 2^n - 1$. Функция $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ вида $F(y) = ay^i + by^j + c$, где $a, b, c \in \mathbb{F}_{2^n}$, $a \neq 0$, $b \neq 0$, $1 \leq i, j \leq 2^n - 1$, $i \neq j$, называется *биномиальной*.

Функция $\text{tr}: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ вида $\text{tr}(y) = y + y^2 + \dots + y^{2^{n-1}}$ называется *следом* элемента $y \in \mathbb{F}_{2^n}$. Примечательность этой функции заключается в том, что для любого y значение $\text{tr}(y)$ будет принадлежать простому подполю \mathbb{F}_2 . Множество $\mathbb{F}_{2^n} \setminus \{0\}$ будем обозначать через $\mathbb{F}_{2^n}^*$.

Следующие утверждения хорошо известны из курса алгебры.

Утверждение 1. Пусть \mathbb{F}_{2^n} — конечное поле из 2^n элементов. Для любого элемента $a \in \mathbb{F}_{2^n}$ выполнено $a^{2^n} = a$.

Утверждение 2. Пусть \mathbb{F}_{2^n} — конечное поле из 2^n элементов, α — примитивный элемент поля. Для любого ненулевого элемента $a \in \mathbb{F}_{2^n}$ существует целое число $1 \leq k \leq 2^n - 1$ такое, что $a = \alpha^k$.

Утверждение 3 (об автоморфизме Фробениуса). Рассмотрим конечное поле \mathbb{F}_{2^n} , где n — натуральное число. Отображение $\phi: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ вида $\phi(a) = a^2$, где $a \in \mathbb{F}_{2^n}$, является автоморфизмом поля. Множество

неподвижных точек этого автоморфизма является простым подполем \mathbb{F}_2 поля \mathbb{F}_{2^n} .

Утверждение 4. Любая линейная функция $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ имеет вид

$$F(x) = \sum_{k=0}^{n-1} a_k x^{2^k}, \quad a_i \in \mathbb{F}_{2^n}.$$

Следующие утверждения можно найти в [15, 16].

Утверждение 5. Функция $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ вида

$$F(y) = a_0 + \sum_{k=1}^{2^n-1} a_k y^k, \quad a_i \in \mathbb{F}_{2^n},$$

принимает значения только из поля \mathbb{F}_2 тогда и только тогда, когда для любого i

$$a_{2i \bmod (2^n-1)} = a_i^2.$$

Утверждение 6. Пусть задана функция $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ вида

$$F(y) = a_0 + \sum_{k=1}^{2^n-1} a_k y^k, \quad a_i \in \mathbb{F}_{2^n}.$$

Её алгебраическая степень равна максимальному весу показателя i степени монома с коэффициентом a_i , отличным от нуля.

2. Взаимно однозначные векторные булевы функции

Данный раздел посвящён изучению взаимно однозначных векторных булевых функций. Рассмотрены биномиальные функции, получено необходимое условие их существования. Исследован вопрос существования биномиальных функций при различных n .

2.1. Мономиальные функции. Мономиальные функции — самый простой класс векторных булевых функций в полиномиальном представлении. Для этого случая свойство взаимной однозначности полностью исследовано. Мономиальные функции $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ имеют вид $F(y) = ay^k + b$, где $a, b \in \mathbb{F}_{2^n}$, $a \neq 0$ и $1 \leq k \leq 2^n - 1$. Заметим, что коэффициент b не влияет на свойство взаимной однозначности, поэтому будем рассматривать функции вида $F(y) = ay^i$, где $a \in \mathbb{F}_{2^n}$, $a \neq 0$. Широко известен следующий факт, который для полноты изложения приведём с доказательством.

Утверждение 7. Функция $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ вида $F(x) = ay^i$, $a \in \mathbb{F}_{2^n}$, $a \neq 0$, взаимно однозначна тогда и только тогда, когда $\gcd(i, 2^n - 1) = 1$.

Доказательство. НЕОБХОДИМОСТЬ. Пусть α — примитивный элемент поля \mathbb{F}_{2^n} . Предположим, что $\gcd(i, 2^n - 1) = m$, $m > 1$. Тогда по утверждению 1 элементы поля α и $\alpha^{1+\frac{2^n-1}{m}}$ перейдут под действием функции F в один элемент поля, а следовательно, функция не будет взаимно однозначной.

ДОСТАТОЧНОСТЬ. Предположим, что функция не взаимно однозначна, т. е. существуют два различных элемента поля α^k и α^m такие, что $\alpha^{ki} = \alpha^{mi}$, где α — примитивный элемент поля \mathbb{F}_{2^n} . Это равенство эквивалентно сравнению $ki \equiv mi \pmod{2^n - 1}$. Так как $\gcd(i, 2^n - 1) = 1$, имеет место сравнение $k \equiv m \pmod{2^n - 1}$. Утверждение 7 доказано.

Мономиальные функции хорошо изучены. Известно шесть классов мономиальных APN-функций $f(y) = y^d$, которые приведены в табл. 1 [9]. Также существует пять классов бент-функций, приведённых в табл. 2, которые являются линейными проекциями мономиальных векторных булевых функций [19, 27].

Таблица 1

Известные показатели мономиальных APN-функций

Функция	Показатель d	Условия
Gold	$2^t + 1$	$\gcd(t, n) = 1$
Kasami	$2^{2t} - 2^t + 1$	$\gcd(t, n) = 1$
Welch	$2^t + 3$	$n = 2t + 1$
Niho	$2^t + 2^{\frac{t}{2}} - 1$, если t чётно $2^t + 2^{\frac{3t+1}{2}} - 1$, если t нечётно	$n = 2t + 1$
Inverse	$d = 2^{2t} - 1$	$n = 2t + 1$
Gold	$d = 2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$

2.2. Биномиальные функции. В общем случае биномиальная функция $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ имеет вид $F(y) = ay^i + by^j + c$, где $a, b, c \in \mathbb{F}_{2^n}$, $a \neq 0$, $b \neq 0$, $1 \leq i, j \leq 2^n - 1$, $i \neq j$. Следует заметить, что свободный коэффициент c не влияет на свойство взаимной однозначности, поэтому достаточно исследовать функции вида $F(y) = ay^i + by^j$.

Функция $b^{-1}F$ взаимно однозначна тогда и только тогда, когда F взаимно однозначна. Поэтому будем исследовать функции вида $F(y) = \alpha^k y^i + y^j$, где $1 \leq k, i, j \leq 2^n - 1$, $i \neq j$, где α — примитивный элемент поля \mathbb{F}_{2^n} . Без ограничения общности можно считать, что $i > j$.

Т а б л и ц а 2

Известные показатели мономиальных бент-функций,
представимых в виде $f(y) = \text{tr}(ay^d)$

Функция	Показатель d	Условия
Dillon	$2^{\frac{n}{2}} - 1$	$\frac{n}{\gcd(n,i)}$ чётно
Gold	$2^i + 1$	$\frac{n}{\gcd(n,i)}$ чётно
Kasami	$2^{2k} - 2^k + 1$	$\gcd(k, n) = 1$
Canteaut, Leander	$(2^k + 1)^2$	$n = 4k, k$ нечётно
Canteaut, Charpin, Kyureghyan	$2^{2k} + 2^k + 1$	$n = 6k$

Биномиальные функции также активно изучаются. Например, в [12] приводятся некоторые классы биномиальных APN-функций. Биномиальная функция вида

$$x^{2^s+1} + wx^{2^{ik}+2^{mk}+s}$$

над полем \mathbb{F}_{2^n} является APN-функцией, если выполнены следующие условия [11]:

$$\begin{aligned} n &= 4k, \quad \gcd(k, 2) = \gcd(s, 2k) = 1, \\ k &\geq 3, \quad i = sk \bmod 4, \quad m = 4 - i, \\ w &\text{ имеет порядок } 2^{3k} + 2^{2k} + 2^k + 1, \end{aligned}$$

либо если выполнены условия [10]

$$\begin{aligned} n &= 3k, \quad \gcd(k, 3) = \gcd(s, 3k) = 1, \\ k &\geq 4, \quad i = sk \bmod 3, \quad m = 3 - i, \\ w &\text{ имеет порядок } 2^{2k} + 2^k + 1. \end{aligned}$$

В [7] доказано, что если функция $f(x) = ax^n + x$ взаимно однозначна над полем \mathbb{F}_p , где $n > 1$ и $a \in \mathbb{F}_p^*$, p — простое число, то $p - 1 \leq (n - 1) \times (n - 3)$.

2.3. Условия существования взаимно однозначных биномиальных функций. Данный пункт посвящён исследованию существования взаимно однозначных биномиальных функций $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ вида $F(y) = \alpha^k y^i + y^j$, где $1 \leq k \leq 2^n - 1$, $1 \leq j < i \leq 2^n - 1$, при различных значениях n .

Получим необходимое условие взаимной однозначности для функции $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ вида $F(y) = \alpha^k y^i + y^j$.

Теорема 1. Пусть $1 \leq j < i \leq 2^n - 1$, $1 \leq k \leq 2^n - 1$, α — примитивный элемент поля \mathbb{F}_{2^n} . Если функция $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ вида $F(y) = \alpha^k y^i + y^j$ взаимно однозначна, то $\gcd(i - j, 2^n - 1)$ не делит k .

ДОКАЗАТЕЛЬСТВО. Допустим, что $\gcd(i - j, 2^n - 1)$ делит k и функция F взаимно однозначна. Так как F взаимно однозначна, уравнение $F(y) = 0$ имеет один корень. Очевидно, что 0 является корнем этого уравнения. Покажем, что уравнение $F(y) = 0$ имеет ещё один корень. Будем искать его в виде α^m , где $1 \leq m \leq 2^n - 1$. Подставив $y = \alpha^m$ в уравнение $f(y) = 0$, получим

$$F(\alpha^m) = \alpha^{k+mi} + \alpha^{mj} = 0.$$

Данное соотношение верно, если

$$k + mi \equiv mj \pmod{2^n - 1},$$

или

$$m(j - i) \equiv k \pmod{2^n - 1}.$$

Последнее сравнение разрешимо, поскольку по предположению $\gcd(i - j, 2^n - 1)$ делит k . Следовательно, функция f не взаимно однозначна. Значит, полученное условие — $\gcd(i - j, 2^n - 1)$ не делит k — является необходимым. Теорема 1 доказана.

Следствие 1. Пусть $1 \leq j < i \leq 2^n - 1$, $1 \leq k \leq 2^n - 1$, α — примитивный элемент поля \mathbb{F}_{2^n} . Если $2^n - 1$ простое, то взаимно однозначных функций $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ вида $F(y) = \alpha^k y^i + y^j$ не существует.

ДОКАЗАТЕЛЬСТВО. Действительно, $\gcd(i - j, 2^n - 1) = 1$. Следовательно, $\gcd(i - j, 2^n - 1)$ делит k , и по теореме 1 функция F не является взаимно однозначной. Следствие 1 доказано.

Для того чтобы доказать существование биномиальных функций в случае составного n , нам потребуется ввести класс линейных функций в полиномиальном представлении и доказать несколько утверждений для него.

По утверждению 4 любая линейная функция $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ имеет вид

$$F(y) = \sum_{k=0}^{n-1} a_k y^{2^k}, \quad a_i \in \mathbb{F}_{2^n}.$$

Лемма 1. Любая линейная функция $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ взаимно однозначна тогда и только тогда, когда уравнение $F(y) = 0$ имеет один корень.

ДОКАЗАТЕЛЬСТВО. НЕОБХОДИМОСТЬ очевидна. Докажем ДОСТАТОЧНОСТЬ. Пусть уравнение $F(y) = 0$ имеет один корень и $F(a) = F(b)$. Тогда $F(a) - F(b) = 0$. Далее, $F(a - b) = 0$ в силу линейности. Так как по условию у уравнения $F(y) = 0$ один корень, то $a - b = 0$. В итоге $a = b$. Лемма 1 доказана.

Теперь рассмотрим линейные функции $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ вида $F(y) = \alpha^k y^{2^m} + y^{2^t}$ и на основе теоремы 1 и леммы 1 докажем

Следствие 2. Пусть $0 < t < m \leq n - 1$, $1 \leq k \leq 2^n - 1$, α — примитивный элемент поля \mathbb{F}_{2^n} . Функция вида $F(y) = \alpha^k y^{2^m} + y^{2^t}$, где k такое, что $\gcd(2^{m-t} - 1, 2^n - 1)$ не делит k , взаимно однозначна.

ДОКАЗАТЕЛЬСТВО. Заметим, что

$$\gcd(2^m - 2^t, 2^n - 1) = \gcd(2^t(2^{m-t} - 1), 2^n - 1) = \gcd(2^{m-t} - 1, 2^n - 1).$$

Так как $\gcd(2^{m-t} - 1, 2^n - 1)$ не делит k , аналогично доказательству теоремы 1 получаем, что уравнение $F(y) = 0$ имеет один корень. Поскольку функция F линейна, в силу леммы 1 она взаимно однозначна. Следствие 2 доказано.

Следующая теорема показывает существование взаимно однозначных функций при составном n .

Теорема 2. Пусть $1 \leq j < i \leq 2^n - 1$, $1 \leq k \leq 2^n - 1$ и α — примитивный элемент поля \mathbb{F}_{2^n} . Если n — составное число, то каждая функция

$$F(y) = \alpha y^{2^{m+k}} + y^{2^k},$$

где $0 \leq k \leq n - m - 1$ и m делит n , взаимно однозначна.

ДОКАЗАТЕЛЬСТВО. Пусть n имеет вид $n = mr$, где $m > 1$, $r > 1$. В этом случае $2^{mr} - 1 = (2^m - 1)(2^{m(r-1)} + 2^{m(r-2)} + \dots + 1)$. Рассмотрим функцию $F(y) = \alpha y^{2^{m+k}} + y^{2^k}$, где $0 \leq k \leq n - m - 1$. Поскольку $\gcd(2^{m+k} - 2^k, 2^n - 1) = 2^m - 1 > 1$, по следствию 2 каждая такая функция взаимно однозначна. Теорема 2 доказана.

Остаётся недоказанным существование взаимно однозначных биномиальных функций при простом n и составном $2^n - 1$ одновременно. В случае, если $2^n - 1$ имеет относительно небольшой делитель, существование биномиальной взаимно однозначной векторной булевой функции от n переменных можно доказать, опираясь на следующее утверждение, полученное в [23].

Утверждение 8 [23]. Пусть \mathbb{F}_q — конечное поле порядка q и заданы целые числа $0 \leq j < i \leq q$ такие, что

$$\gcd(i, j, q-1) = 1, \quad \gcd(i-j, q-1) > \frac{2q \log_{10} \log_{10} q}{\log_{10} q}.$$

Тогда существует такое $a \in \mathbb{F}_q^*$, что функция $F: \mathbb{F}_q \rightarrow \mathbb{F}_q$, имеющая вид $F(y) = ay^i + y^j$, взаимно однозначна.

Теорема 3. Если $2^n - 1$ имеет делитель $d < \frac{(2^n-1)n}{2^{n+1}\log_2 n}$, то существует взаимно однозначная функция $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ вида $F(y) = ay^i + y^j$ для некоторого $a \in \mathbb{F}_{2^n}^*$, $0 < j < i < 2^n - 1$.

ДОКАЗАТЕЛЬСТВО. Преобразуем оценку утверждения 8 для случая $q = 2^n$. Распишем $2^n - 1 = Md$ — произведение двух чисел $d > 1$, $M > 1$, где d как минимальный простой делитель, M — оставшийся множитель соответственно. Имеем

$$\begin{aligned} \frac{2q \log_{10} \log_{10} q}{\log_{10} q} &= \frac{2^{n+1} \log_2 10 (\log_{10} n - \log_{10} \log_2 10)}{n} \\ &= \frac{2^{n+1} (\log_2 n - \log_2 \log_2 10)}{n}. \end{aligned}$$

Выберем в качестве i, j такие числа, что значение $\gcd(i-j, 2^n - 1)$ максимально, т. е. равно M . Получим

$$M > \frac{2^{n+1} (\log_2 n - \log_2 \log_2 10)}{n}.$$

Тогда для любого $M > \frac{2^{n+1} \log_2 n}{n}$ условие утверждения 8 будет выполнено. Перепишем это неравенство относительно делителя d . Получим ограничение $d < \frac{(2^n-1)n}{2^{n+1}\log_2 n}$. Теорема 3 доказана.

Можно задать ограничения на степени мономов биномиальной функции, используя следующее утверждение, доказанное в [24] и улучшенное в [28].

Утверждение 9 [24]. Пусть $q = p^m$, где p — простое число, $m > 0$. Если функция $F(x) = ay^i + y^j$ взаимно однозначна над полем \mathbb{F}_q , где $i > j > 0$ и $a \in \mathbb{F}_q^*$, то $q \leq (i-2)^4 + 4i - 4$ или $i = jp^m$.

Для случая $q = 2^p$ получаем

Следствие 3. Пусть p простое и $p > 3$. Если функция $F: \mathbb{F}_{2^p} \rightarrow \mathbb{F}_{2^p}$ вида $F(x) = \alpha^k x^i + x^j$ взаимно однозначна, то либо $i \geq 2^{p/4} + 1$, либо $\gcd(j, 2^p - 1)$ не делит k .

ДОКАЗАТЕЛЬСТВО. Используя утверждение 9, имеем $2^p \leq (i-2)^4 + 4i - 4$. Если разрешить данное неравенство, то получим $i \geq \lceil 2^{p/4} + 1 \rceil$. В случае $i = j2^m$ можно использовать теорему 1. Если функция F взаимно однозначна, то $\gcd(i-j, 2^p-1) = \gcd(j(2^m-1), 2^p-1)$ не делит k . Хорошо известен следующий факт: если p простое, то $\gcd(2^m-1, 2^p-1) = 1$ для всех $0 < m < p$. Стало быть, $\gcd(j, 2^p-1)$ не делит k . Следствие 3 доказано.

2.4. Общий вид взаимно однозначных функций. Общий случай взаимно однозначных векторных булевых функций в полиномиальном представлении $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ остаётся наименее исследованным. В этом пункте приведены известные утверждения, которые формулируются для общего представления в виде полинома

$$F(y) = a_0 + \sum_{k=1}^{2^n-1} a_k y^k, \quad a_i \in \mathbb{F}_{2^n}.$$

Следующее утверждение является известным результатом для взаимно однозначных функций в полиномиальном представлении [22].

Утверждение 10 (критерий Эрмита). Пусть $q = p^n$, где p — простое, а n — натуральное число. Функция $F: \mathbb{F}_q \rightarrow \mathbb{F}_q$ взаимно однозначна тогда и только, когда выполняются два условия:

- (1) $F(x)^{q-1} \bmod (x^q - x)$ является полиномом степени $q-1$;
- (2) для любого t такого, что $1 \leq t \leq q-2$ и $t \not\equiv 0 \pmod{p}$ полином $F(x)^t \bmod (x^q - x)$ имеет степень не больше $q-2$.

Следующее утверждение формулирует один из методов построения взаимно однозначных векторных булевых функций в полиномиальном представлении.

Утверждение 11 [29]. Пусть $h > 0$ таково, что $\gcd(h, q-1) = 1$, и s делит $q-1$. Пусть функция $g: \mathbb{F}_q \rightarrow \mathbb{F}_q$ не имеет ненулевых корней. Тогда функция $f: \mathbb{F}_q \rightarrow \mathbb{F}_q$ вида $f(x) = x^h(g(x^s))^{\frac{q-1}{s}}$ взаимно однозначна.

3. Вычислительный эксперимент

В данном разделе представлены результаты поиска взаимно однозначных биномиальных функций $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ вида $F(y) = ay^i + y^j$ и исследования их криптографических свойств при $n \leq 8$.

3.1. Ограничения на поиск. Для начала без ввода ограничений необходимо проверить свойство взаимной однозначности у каждой функции вида $F(y) = ay^i + y^j$, т. е. нужно просмотреть $(2^n - 1)^3$ функций.

Если воспользоваться теоремой 1, то можно проверять только такие функции, для которых $\gcd(i - j, 2^n - 1) > 1$. В этом случае число рассматриваемых функций становится равным

$$(2^n - 1) \sum_{p|2^n-1} \sum_{i=1}^{2^n-1} \left\lfloor \frac{i}{p} \right\rfloor.$$

Поясним полученную формулу. Коэффициент a функции $F(y) = ay^i + y^j$ можно выбрать $2^n - 1$ способами. При фиксированном i нужно перебрать все такие j , что $i - j$ и $2^n - 1$ имеют общий делитель больше 1. Можно проверять такие i, j , что $(i - j)$ и $2^n - 1$ имеют один и тот же простой делитель. Получается, что при фиксированном i и простом делителе p числа $2^n - 1$ количество способов выбрать число j равно $\left\lfloor \frac{i}{p} \right\rfloor$.

Также при переборе учитываются автоморфизмы Фробениуса (утверждение 3). Из множества $\{ay^i + y^j, a^2y^{2i} + y^{2j}, \dots, a^{2^{n-1}}y^{2^{n-1}i} + y^{2^{n-1}j}\}$ будет рассматриваться только одна функция, на которой достигается минимум среди максимумов показателей степеней её мономов.

3.2. Результаты вычислений. Из теоремы 1 и следствия 1 вытекает, что в случае простого числа $2^n - 1$ взаимно однозначных функций $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ вида $F(y) = ay^i + y^j$ не существует, поэтому при $n = 2, 3, 5, 7$ функций такого вида нет.

В следующих утверждениях приведены результаты вычислений с учётом ограничений п. 3.1. Все использованные неприводимые многочлены взяты из [26].

Утверждение 12. Любая взаимно однозначная биномиальная функция над полем \mathbb{F}_{2^4} имеет вид

$$ax^4 + x^1 \quad \text{или} \quad ax^{13} + x^7,$$

$a \in \{2, 3, 4, 5, 6, 7, 9, 11, 13, 14\} \subset \mathbb{F}_{2^4}$, где поле \mathbb{F}_{2^4} построено с помощью неприводимого полинома $x^4 + x + 1$.

Утверждение 13. Любая взаимно однозначная биномиальная функция над полем \mathbb{F}_{2^6} имеет один из следующих видов:

- $ay^{55} + y^{31}, ay^{29} + y^{23}, ay^{25} + y^{22}, ay^{19} + y^{13}, ay^{17} + y^5, ay^4 + y^1$,
 $a \in \{2, 4, 6, 7, 9, 10, 11, 12, 16, 19, 20, 21, 26, 27, 28, 29, 30, 31, 32, 33,$
 $34, 35, 36, 37, 38, 39, 41, 42, 44, 45, 46, 47, 48, 49, 50, 52, 53, 55, 56, 60,$
 $61\} \subset \mathbb{F}_{2^6}$;
- $ay^{47} + y^{29}, ay^{38} + y^{29}, ay^{31} + y^{22}, ay^{20} + y^{11}, ay^{13} + y^4, ay^{10} + y^1$,
 $a \in \{3, 5, 8, 13, 17, 18, 40, 43, 51, 54, 57, 58, 59, 62\} \subset \mathbb{F}_{2^6}$;

- $ay^{52} + y^{31}$, $ay^{43} + y^{22}$, $ay^{34} + y^{13}$, $ay^{31} + y^{10}$, $ay^{22} + y^1$, $a \in \{6, 11, 15, 20, 22, 24, 26, 28, 31, 40, 43, 51, 54, 57, 62\} \subset \mathbb{F}_{2^6}$;
- $ay^{47} + y^{26}$, $ay^{44} + y^{23}$, $ay^{32} + y^{11}$, $ay^{26} + y^5$, $ay^{23} + y^2$, $a \in \{3, 5, 6, 8, 11, 13, 14, 17, 18, 20, 23, 25, 26, 28, 31\} \subset \mathbb{F}_{2^6}$;
- $ay^{59} + y^{31}$, $ay^{43} + y^{29}$, $ay^{26} + y^{19}$, $ay^{25} + y^{11}$, $ay^{17} + y^{10}$, $ay^8 + y^1$, $a \in \{2, 3, 4, 5, 7, 8, 9, 10, 12, 13, 14, 15, 16, 17, 18, 19, 21, 22, 23, 24, 25, 27, 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 60, 61, 62\} \subset \mathbb{F}_{2^6}$,

где поле \mathbb{F}_{2^6} построено с помощью неприводимого полинома $x^6 + x + 1$.

Утверждение 14. Любая взаимно однозначная биномиальная функция над полем \mathbb{F}_{2^8} имеет один из следующих видов:

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

234, 235, 236, 237, 238, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254} $\subset \mathbb{F}_{2^8}$;

• $ay^{178} + y^{127}$, $ay^{158} + y^{107}$, $ay^{113} + y^{62}$, $ay^{103} + y^{52}$, $ay^{98} + y^{47}$, $ay^{73} + y^{22}$, $ay^{58} + y^7$, $ay^{53} + y^2$, $a \in \{13, 81, 92, 93, 177, 188, 189, 224, 225, 236\} \subset \mathbb{F}_{2^8}$;

• $ay^{191} + y^{106}$, $ay^{179} + y^{94}$, $ay^{122} + y^{37}$, $ay^{116} + y^{31}$, $ay^{107} + y^{22}$, $ay^{98} + y^{13}$, $ay^{92} + y^7$, $ay^{86} + y^1$, $a \in \{15, 22, 33, 35, 36, 62, 71, 83, 85, 89, 96, 101, 105, 109, 110, 117, 124, 126, 129, 132, 134, 136, 138, 140, 142, 144, 147, 149, 150, 155, 161, 166, 172, 181, 185, 190, 196, 199, 202, 205, 206, 214, 218, 222, 226, 241, 247, 252\} \subset \mathbb{F}_{2^8}$;

• $ay^{207} + y^{122}$, $ay^{192} + y^{107}$, $ay^{171} + y^{86}$, $ay^{147} + y^{62}$, $ay^{144} + y^{59}$, $ay^{138} + y^{53}$, $ay^{132} + y^{47}$, $ay^{126} + y^{41}$, $ay^{123} + y^{38}$, $ay^{114} + y^{29}$, $ay^{111} + y^{26}$, $ay^{108} + y^{23}$, $ay^{99} + y^{14}$, $ay^{96} + y^{11}$, $ay^{87} + y^2$, $a \in \{8, 15, 22, 29, 32, 33, 35, 51, 58, 62, 64, 74, 83, 85, 101, 105, 106, 108, 109, 114, 128, 129, 131, 134, 142, 144, 145, 148, 149, 150, 151, 154, 155, 159, 161, 171, 179, 181, 196, 197, 206, 212, 214, 216, 232, 239, 247, 252\} \subset \mathbb{F}_{2^8}$;

• $ay^{211} + y^{126}$, $ay^{208} + y^{123}$, $ay^{196} + y^{111}$, $ay^{172} + y^{87}$, $ay^{148} + y^{63}$, $ay^{142} + y^{57}$, $ay^{139} + y^{54}$, $ay^{127} + y^{42}$, $ay^{124} + y^{39}$, $ay^{112} + y^{27}$, $ay^{106} + y^{21}$, $ay^{103} + y^{18}$, $ay^{94} + y^9$, $ay^{91} + y^6$, $ay^{88} + y^3$, $a \in \{8, 29, 32, 36, 51, 58, 64, 71, 74, 89, 96, 106, 108, 110, 114, 117, 124, 126, 128, 131, 132, 136, 138, 140, 145, 147, 148, 151, 154, 159, 166, 171, 172, 179, 185, 190, 197, 199, 202, 205, 212, 216, 218, 222, 226, 232, 239, 241\} \subset \mathbb{F}_{2^8}$,

где поле \mathbb{F}_{2^8} построено с помощью неприводимого полинома $x^8 + x^4 + x^3 + 1$.

Среди рассмотренных функций при $n \in \{6, 8\}$ был выполнен поиск APN-функций и дифференциально 4-равномерных функций. Результаты поиска отражены в следующих трёх утверждениях.

Утверждение 15. Над полями \mathbb{F}_{2^6} и \mathbb{F}_{2^8} не существует взаимно однозначных биномиальных APN-функций.

Утверждение 16. Любая взаимно однозначная биномиальная дифференциально 4-равномерная функция над полем \mathbb{F}_{2^6} имеет один из следующих видов:

$$ay^{55} + y^{31}, \quad ay^{19} + y^{13}, \quad ay^{17} + y^5,$$

$a \in \{2, 4, 6, 7, 9, 10, 11, 12, 16, 19, 20, 21, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 41, 42, 44, 45, 46, 47, 48, 49, 50, 52, 53, 55, 56, 60, 61\} \subset \mathbb{F}_{2^6}$, где поле \mathbb{F}_{2^6} построено с помощью неприводимого полинома $x^6 + x + 1$.

Утверждение 17. Любая взаимно однозначная биномиальная дифференциально 4-равномерная функция от 8 переменных над полем \mathbb{F}_{2^8} имеет вид

$$ay^{247} + y^{127},$$

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

Важное криптографическое свойство векторных булевых функций — высокая компонентная алгебраическая иммунность. Данное понятие было введено в [14] и рассматривалось, например, в [3]. Среди найденных функций (предложения 12, 13) при $n = 4, 6$ было посчитано количество взаимно однозначных биномиальных функций с максимальной компонентной алгебраической иммунностью. При $n = 4$ их число равно 10, а при $n = 6$ число таких функций уже равно 319. При $n = 8$ была найдена функция $f(y) = 2y^{223} + y^{127}$ с максимальной компонентной алгебраической иммунностью 4, однако проверить все функции при $n = 8$ пока не удалось.

4. Заключение

В работе исследованы взаимно однозначные биномиальные функции, сформулировано и доказано необходимое условие взаимной однозначности биномиальной функции и исследован вопрос существования таких функций при различных условиях на n и $2^n - 1$. Кроме того, построены все биномиальные взаимно однозначные функции при $n \leq 8$, исследовано свойство дифференциальной равномерности полученного списка взаимно однозначных биномиальных функций. Найдены все дифференциально 4-равномерные функции от 6 и 8 переменных и взаимно однозначные

биномиальные функции с максимальной компонентной алгебраической иммунностью при $n = 4, 6, 8$. Остаётся открытым вопрос существования взаимно однозначных биномиальных функций в случае, если $2^n - 1$ не имеет достаточно малого делителя. В будущем предлагается исследовать этот случай и начать изучение функций, которые могут быть представлены в виде суммы трёх мономов.

Автор выражает благодарность Н. Н. Токаревой и А. А. Городиловой за ценные советы при планировании исследования и рекомендации по оформлению статьи.

ЛИТЕРАТУРА

1. Глухов М. М. О приближении дискретных функций линейными функциями // Мат. вопросы криптографии. 2016. Т. 7, № 4. С. 29–50.
2. Городилова А. А. От криптоанализа шифра к криптографическому свойству булевой функции // Прикл. дискрет. математика. 2016. № 3. С. 16–44.
3. Покрасенко Д. П. О максимальной компонентной алгебраической иммунности векторных булевых функций // Дискрет. анализ и исслед. операций. 2016. Т. 23, № 2. С. 88–99.
4. Сачков В. Н. Комбинаторные свойства дифференциально 2-равномерных подстановок // Мат. вопросы криптографии. 2015. Т. 6, № 1. С. 159–179.
5. Токарева Н. Н. Симметричная криптография. Краткий курс. Новосибирск: Новосиб. гос. ун-т, 2012. 234 с.
6. Тужилин М. Э. Почти совершенные нелинейные функции // Прикл. дискрет. математика. 2009. № 3. С. 14–20.
7. Ayad M., Belghaba K., Kihel O. On permutation binomials over finite fields // Bull. Aust. Math. Soc. 2014. No. 89. P. 112–124.
8. Bracken C., Byrne E., Markin N., McGuire G. Fourier spectra of Binomial APN functions // SIAM J. Discrete Math. 2008. Vol. 23, No. 2. P. 596–608.
9. Budaghyan L. Construction and analysis of cryptographic functions // Berlin: Springer-Verl., 2015. 176 p.
10. Budaghyan L., Carlet C., Felke P., Leander G. An infinite class of quadratic APN functions which are not equivalent to power mappings // Proc. 17th IEEE Int. Symp. Information Theory (Seattle, USA, July 9–14, 2006). Piscataway: IEEE, 2006. P. 2637–2641.
11. Budaghyan L., Carlet C., Leander G. Another class of quadratic APN binomials over \mathbb{F}_{2^n} : the case n divisible by 4 // Proc. Int. Workshop Coding Cryptography (WCC 2007). (Versailles, France, Apr. 16–20, 2007). P. 49–58.

12. **Budaghyan L., Carlet C., Leander G.** Constructing new APN functions from known ones // *Finite Fields Appl.* 2009. Vol. 15, No. 2. P. 150–159.
13. **Canteaut A., Charpin P., Kyureghyan G.** A new class of monomial bent functions // *Finite Fields Appl.* 2008. Vol. 14, № 1. P. 221–241.
14. **Carlet C.** On the algebraic immunities and higher order nonlinearities of vectorial Boolean functions // *Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes. Proc. NATO Adv. Res. Workshop ACPTECC (Veliko Tarnovo, Bulgaria, Oct. 6–9, 2008).* Amsterdam: IOS Press, 2009. P. 104–116.
15. **Carlet C.** Boolean functions for cryptography and error-correcting codes // *Boolean models and methods in mathematics, computer science, and engineering.* New York: Camb. Univ. Press, 2010. P. 257–397. (*Encycl. Math. Its Appl.*; Vol. 134).
16. **Carlet C.** Vectorial Boolean functions for cryptography // *Boolean Models and Methods in Mathematics, Computer Science, and Engineering.* New York: Camb. Univ. Press, 2010. P. 398–470. (*Encycl. Math. Its Appl.*; Vol. 134).
17. **Daemen J., Rijmen V.** AES Proposal: Rijndael. Belgium, 1999.
18. **Daemen J., Rijmen V.** The design of Rijndael. Heidelberg: Springer, 2002. 238 p.
19. **Dobbertin H.** Almost perfect nonlinear power functions on \mathbb{F}_{2^n} : the Welch case // *IEEE Trans. Inf. Theory.* 1999. Vol. 45, No. 4. P. 1271–1275.
20. **Dobbertin H., Leander G.** A survey of some recent results on bent functions // *Sequences and Their Applications – SETA 2004. Rev. Sel. Papers 3rd Int. Conf. (Seoul, Korea, Oct. 24–28, 2004).* Heidelberg: Springer, 2005. P. 1–29. (*Lect. Notes Comput. Sci.*; Vol. 3486).
21. **Dobbertin H., Leander G., Canteaut A., Carlet C., Felke P., Gaborit P.** Construction of bent functions via Niho power functions // *J. Comb. Theory. Ser. A.* 2006. Vol. 113, No. 5. P. 779–798.
22. **Hou X.** Permutation polynomials over finite fields — A survey of recent advances // *Finite Fields Their Appl.*, 2015. Vol. 32. P. 82–119.
23. **Masuda A. M., Zieve M. E.** Permutation binomials over finite fields // *Trans. Am. Math. Soc.* 2009. Vol. 361, No. 8. P. 4169–4180.
24. **Niederreiter H., Robinson K.** Complete mappings of finite fields // *J. Aust. Math. Soc.* 1982. Vol. 33, No. 2. P. 197–212.
25. **Nyberg K.** Differentially uniform mappings for cryptography // *Advances in Cryptology (EUROCRYPT'93). Proc. Workshop Theory Appl. Crypt. Tech. (Lofthus, Norway, May 23–27, 1993).* Heidelberg: Springer, 1994. (*Lect. Notes Comput. Sci.*; Vol. 765).
26. **Seroussi G.** Table of low-weight binary irreducible polynomials. Tech. Rep. HPL-98-135. Hewlett-Packard, 1998.
27. **Tokareva N. N.** Bent functions: Results and applications to cryptography. London: Acad. Press, 2015. 220 p.

-
28. **Turnwald G.** Permutation polynomials of binomial type // Contributions to general algebra. Vienna: Holder–Pichler–Tempsky, 1988. Vol. 6. 281–286.
29. **Shallue C. J.** Permutation polynomials of finite fields // Honours project. Monash University, 2012.
30. **Yang M., Meng Q., Zhang H.** Evolutionary design of trace form bent functions // Cryptology ePrint Arch. Rep. 2005/322. <https://eprint.iacr.org/2005/322>.

Милосердов Алексей Васильевич

Статья поступила
20 февраля 2018 г.

Исправленный вариант —
4 июня 2018 г.

PERMUTATION BINOMIAL FUNCTIONS OVER FINITE FIELDS

A. V. Miloserdov

Novosibirsk State University,
1 Pirogov St., 630090 Novosibirsk, Russia

E-mail: amiloserdov6@gmail.com

Abstract. We consider binomial functions over a finite field of order 2^n . Some necessary condition is found for such a binomial function to be a permutation. It is proved that there are no permutation binomial functions in the case that $2^n - 1$ is prime. Permutation binomial functions are constructed in the case when n is composite and found for $n \leq 8$. Tab. 2, bibliogr. 30.

Keywords: vectorial Boolean function, binomial function, permutation, APN function.

REFERENCES

1. M. M. Glukhov, On the approximation of discrete functions by linear functions, *Mat. Vopr. Kriptogr.*, **7**, No. 4, 29–50, 2016 [Russian].
2. A. A. Gorodilova, From cryptanalysis to cryptographic property of a Boolean function, *Prikl. Diskretn. Mat.*, No. 3, 16–44, 2016 [Russian].
3. D. P. Pokrasenko, On the maximal component algebraic immunity of vectorial Boolean functions, *Diskretn. Anal. Issled. Oper.*, **23**, No. 2, 88–99, 2016 [Russian]. Translated in *J. Appl. Ind. Math.*, **10**, No. 2, 257–263, 2016.
4. V. N. Sachkov, Combinatorial properties of differentially 2-uniform substitutions, *Mat. Vopr. Kriptogr.*, **6**, No. 1, 159–179, 2015 [Russian].
5. N. N. Tokareva, *Symmetric Cryptography: A Brief Course*, Novosib. Gos. Univ., Novosibirsk, 2012 [Russian].
6. M. E. Tuzhilin, APN-functions, *Prikl. Diskretn. Mat.*, No. 3, 14–20, 2009 [Russian].
7. M. Ayad, K. Belghaba, and O. Kihel, On permutation binomials over finite fields, *Bull. Aust. Math. Soc.*, **89**, No. 1, 112–124, 2014.
8. C. Bracken, E. Byrne, N. Markin, and G. McGuire, Fourier spectra of binomial APN functions, *SIAM J. Discrete Math.*, **23**, No. 2, 596–608, 2009.
9. L. Budaghyan, *Construction and Analysis of Cryptographic Functions*, Springer, Cham, 2015.

10. **L. Budaghyan, C. Carlet, P. Felke, and G. Leander**, An infinite class of quadratic APN functions which are not equivalent to power mappings, in *Proc. 17th IEEE Int. Symp. Inf. Theory, Seattle, USA, July 9–14*, pp. 2637–2641, IEEE, Piscataway, 2006.
11. **L. Budaghyan, C. Carlet, and G. Leander**, Another class of quadratic APN binomials over \mathbb{F}_{2^n} : The case n divisible by 4, in *Proc. Int. Workshop Coding Cryptogr., Versailles, France, Apr. 16–20*, pp. 49–58, 2007.
12. **L. Budaghyan, C. Carlet, and G. Leander**, Constructing new APN functions from known ones, *Finite Fields Appl.*, **15**, No. 2, 150–159, 2009.
13. **A. Canteaut, P. Charpin, and G. Kyureghyan**, A new class of monomial bent functions, *Finite Fields Appl.*, **14**, No. 1, 221–241, 2008.
14. **C. Carlet**, On the algebraic immunities and higher order nonlinearities of vectorial Boolean functions, in *Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes* (Proc. NATO Adv. Res. Workshop ACPTECC, Veliko Tarnovo, Bulgaria, Oct. 6–9, 2008), pp. 104–116, IOS Press, Amsterdam, 2009.
15. **C. Carlet**, Boolean functions for cryptography and error-correcting codes, in *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, pp. 257–397, Cambridge Univ. Press, New York, 2010 (Encycl. Math. Its Appl., Vol. 134).
16. **C. Carlet**, Vectorial Boolean functions for cryptography, in *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, pp. 398–472, Cambridge Univ. Press, New York, 2010 (Encycl. Math. Its Appl., Vol. 134).
17. **J. Daemen and V. Rijmen**, AES Proposal: Rijndael, Belgium, 1999.
18. **J. Daemen and V. Rijmen**, *The Design of Rijndael*, Springer, Heidelberg, 2002.
19. **H. Dobbertin**, Almost perfect nonlinear power functions on \mathbb{F}_{2^n} : The Welch case, *IEEE Trans. Inf. Theory*, **45**, No. 4, 1271–1275, 1999.
20. **H. Dobbertin and G. Leander**, A survey of some recent results on bent functions, in *Sequences and Their Applications – SETA 2004* (Revis. Sel. Pap. 3rd Int. Conf., Seoul, Korea, Oct. 24–28, 2004), pp. 1–29, Springer, Heidelberg, 2005 (Lect. Notes Comput. Sci., Vol. 3486).
21. **H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, and P. Gaborit**, Construction of bent functions via Niho power functions, *J. Comb. Theory, Ser. A*, **113**, No. 5, 779–798, 2006.
22. **X. Hou**, Permutation polynomials over finite fields – A survey of recent advances, *Finite Fields Appl.*, **32**, 82–119, 2015.
23. **A. M. Masuda and M. E. Zieve**, Permutation binomials over finite fields, *Trans. Am. Math. Soc.*, **361**, No. 8, 4169–4180, 2009.
24. **H. Niederreiter and K. H. Robinson**, Complete mappings of finite fields, *J. Aust. Math. Soc.*, **33**, No. 2, 197–212, 1982.

- 25. **K. Nyberg**, Differentially uniform mappings for cryptography, in *Advances in Cryptology — EUROCRYPT'93* (Proc. Workshop Theory Appl. Cryptogr. Tech., Lofthus, Norway, May 23–27, 1993), pp. 55–64, Springer, Heidelberg, 1994 (Lect. Notes Comput. Sci., Vol. 765).
- 26. **G. Seroussi**, Table of low-weight binary irreducible polynomials, *Tech. Rep. HPL-98-135*, Hewlett-Packard, 1998.
- 27. **N. N. Tokareva**, *Bent Functions: Results and Applications to Cryptography*, Acad. Press, London, 2015.
- 28. **G. Turnwald**, Permutation polynomials of binomial type, in *Contributions to General Algebra*, Vol. 6, pp. 281–286, Hölder-Pichler-Tempsky, Vienna, 1988.
- 29. **C. J. Shallue**, Permutation polynomials of finite fields, *Honours project*, Monash University, 2012.
- 30. **M. Yang, Q. Meng, and H. Zhang**, Evolutionary design of trace form bent functions, 2005 (Cryptol. ePrint Arch., Rep. 2005/322).

Aleksey V. Miloserdov

Received
20 February 2018
Revised
4 June 2018