Федеральное государственное бюджетное учреждение науки
Институт математики им. С. Л. Соболева
Сибирского отделения Российской академии наук
(ИМ СО РАН)

На правах рукописи
УДК 519.7

Идрисова Валерия Александровна

О построении почти совершенно нелинейных векторных функций и их симметрических свойствах

Специальность 01.01.09 —
«Дискретная математика и математическая кибернетика»

Диссертация на соискание ученой степени
кандидата физико-математических наук

Научный руководитель:
к.ф.-м.н., с.н.с.
Токарева Н.Н.

Новосибирск — 2018

Оглавление

Введение

Область исследования данной работы — векторные булевы функции, которые являются основными нелинейными преобразованиями в криптосистемах с секретным ключом. Изучаются комбинаторные свойства APN-функций, обладающих оптимальной стойкостью к дифференциальному криптоанализу. Предлагаются методы построения новых взаимно однозначных APN-функций. Также исследуются специальные разбиения векторных булевых функций с целью защиты практической реализации алгоритма от атак по сторонним каналам.

Приведем необходимые определения.

Будем обозначать через $\mathbb{F}_2^n$ множество всех двоичных векторов длины n, а через $GF(2^n)$ — конечное поле порядка 2^n. Через $+$, если не сказано иначе, будем обозначать покоординатное сложение векторов из $\mathbb{F}_2^n$ по модулю 2. Для векторов $x = (x_1, \ldots, x_n)$ и $y = (y_1, \ldots, y_n)$ из $\mathbb{F}_2^n$ аналог *скалярного произведения* определяется как $\langle x, y\rangle = x_1y_1 + \ldots + x_ny_n$. Пусть $\mathbf{0} = (0, \ldots, 0)$ — вектор, состоящих из всех нулей, а $\mathbf{1} = (1, \ldots, 1)$ — вектор, состоящих из всех единиц.

Функция F из $\mathbb{F}_2^n$ в $\mathbb{F}_2^m$, где n и m целые числа, называется *векторной булевой функцией*. Если $m = 1$, то функция F называется *булевой*. Произвольная векторная функция F может быть представлена как набор из m *координатных функций* $F = (f_1, \ldots, f_m)$, где f_i — булева функция от n переменных. Для произвольного ненулевого вектора $v \in \mathbb{F}_2^m$ линейная комбинация координатных функций $f_v = v \cdot F$ называется *компонентной функцией*. *Вектором значений* для векторной функции F называется вектор $\big(F(x^{(1)}), \ldots, F(x^{(2^n)})\big)$, где $x^{(1)}, \ldots, x^{(2^n)}$ — лексикографически упорядоченные двоичные векторы из $\mathbb{F}_2^n$.

Вес $\mathrm{wt}(f)$ булевой функции f равен числу единиц в векторе ее значений. *Расстоянием Хэмминга* $\mathrm{d}(f, g)$ между булевыми функциями f и g называется число векторов, на которых значения функций различаются. Расстояние от функции g до множества функций $\mathcal{M}_n$ определяется как $\mathrm{d}(g, \mathcal{M}_n) = \min\{\mathrm{d}(f, g) : f \in \mathcal{M}_n\}$. *Спектр Уолша — Адамара* булевой функции f от n переменных состоит из коэффициентов $W_f(u) = \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+\langle u,x\rangle}$, где $u \in \mathbb{F}_2^n$, где символ минуса используется как знак вещественного числа, а суммирование по всевозможным векторам проводится как обычное сложение вещественных чисел.

Любую векторную булеву функцию F можно единственным образом представить в виде *алгебраической нормальной формы* (АНФ):

$$F(x_1,\dots,x_n)=\sum_{k=1}^{n}\sum_{1\leqslant i_1<\dots<i_k\leqslant n} a_{i_1,\dots,i_k}x_{i_1}\dots x_{i_k}+a_0,$$

где $a_{i_1,\dots,i_k},\ a_0\in\mathbb{F}_2^m$. *Алгебраической степенью* функции F называется количество переменных в самом длинном слагаемом ее АНФ, при котором коэффициент не равен нулю. Если алгебраическая степень F не превышает единицы, то F называется *аффинной*. Аффинная функция F называется *линейной*, если $F(\mathbf{0})=\mathbf{0}$.

Векторная булева функция F называется *уравновешенной*, если она принимает каждое значение из $\mathbb{F}_2^m$ ровно 2^{n-m} раз, в частности, булева функция *уравновешена*, или *сбалансирована*, если она принимает каждое значение 2^{n-1} раз. В случае $n=m$ уравновешенная функция F называется *взаимно однозначной,* или *перестановкой*. *Производной* функции F по направлению a называется векторная функция $D_aF(x)=F(x+a)+F(x)$, где a — ненулевой вектор из $\mathbb{F}_2^n$. Векторная функция F из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$ называется *2-в-1 функцией*, если она принимает 2^{n-1} различных значений, каждое из которых встречается в векторе значений ровно два раза.

Мы можем сопоставить векторному пространству $\mathbb{F}_2^n$ конечное поле $GF(2^n)$ и рассматривать векторную булеву функцию, как функцию над полем $GF(2^n)$. Тогда любая векторная функция F единственным образом представляется над $GF(2^n)$ в следующей форме:

$$F(x)=\sum_{i=0}^{2^n-1}\lambda_i x^i,\ \lambda_j\in GF(2^n).$$

Пусть $F(x)$ и $G(x)$ — векторные функции из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$, тогда будем обозначать через $F\circ G$ *композицию* $F(G(x))$ данных функций. Векторные булевы функции F и G называются *расширенно аффинно эквивалентными (EA-эквивалентными)*, если $F=A_1\circ G\circ A_2+A$, где A_1,A_2 — взаимно однозначные аффинные функции над $\mathbb{F}_2^n$ и A — аффинная функция. Если функции F и G являются EA-эквивалентными и $A\equiv\mathbf{0}$, то F и G называются *аффинно эквивалентными*. Рассмотрим еще одно отношение эквивалентности (см. [36]) на множестве векторных булевых функций. Две функции F и G называются *CCZ-эквивалентными*, если соответствующие множества $\{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n \mid y=F(x)\}$ и $\{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n \mid y=G(x)\}$ являются аффинно эквивалентными, или, ес-

Таблица 1: Известные мономиальные APN-функции вида x^d над полем $GF(2^n)$.

Название	Значение d	Условия	Ссылки
Голда	2^t+1	$(t,n)=1$	[48], [67]
Касами	$2^{2t}-2^t+1$	$(t,n)=1$	[56], [55]
Уолша	2^t+3	$n=2t+1$	[30], [42]
Нихо	$2^t+2^{\frac{t}{2}}-1$, t чётное $2^t+2^{\frac{3t+1}{2}}-1$, t нечётное	$n=2t+1$	[41], [52]
Инверсия	$2^{2t}-1$	$n=2t+1$	[9], [67]
Доббертина	$2^{4t}+2^{3t}+2^{2t}+2^t-1$	$n=5t$	[44]

ли существует аффинный автоморфизм $A=(A_1,A_2)$ такой, что $y=F(x) \Leftrightarrow A_2(x,y)=G(A_1(x,y))$.

Рассмотрим векторную функцию F из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$. Для векторов $a,b \in \mathbb{F}_2^n$, где $a \neq \mathbf{0}$, определим следующую величину:

$$\delta(a,b)=\left|\{\ x \in \mathbb{F}_2^n \ \middle|\ F(x+a)+F(x)=b\}\right|.$$

Обозначим через Δ_F следующий параметр:

$$\Delta_F=\max_{a\neq\mathbf{0},\ b\in\mathbb{F}_2^n}\delta(a,b).$$

Функция F называется *дифференциально Δ_F-равномерной*. Чем меньше параметр Δ_F, тем выше стойкость шифра, содержащего F в качестве S-блока, к дифференциальному криптоанализу. Для векторных функций из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$ наименьшее значение Δ_F равно 2. В этом случае функция F называется *почти совершенно нелинейной (APN-функцией)*. Данные понятия были введены К. Ньюберг в работе [67]. Если F является APN-функцией, то любая EA-эквивалентная/CCZ-эквивалентная функция также является APN-функцией.

Наиболее известные представители класса APN-функций — это мономиальные функции, то есть функции вида $F(x)=x^d$ (см. Таблицу 1) над конечным полем $GF(2^n)$. Известно (см. [1]), что APN-функции изучались еще в СССР, так, например, в 1964 году В. А. Башевым и Б. А. Егоровым было доказано, что мономиальная функция $F(x)=x^{2^{2t}-1}$ является APN-функцией при $n=2t+1$. Исследованию APN-функций посвящено большое число работ как российских авторов: М. М. Глухов, В. А. Зиновьев, В. Н. Сачков, М. Э. Тужилин, Д. Г. Фон-дер-Флаасс, А. А. Городилова и др.; так и зарубежных: L. Budaghyan, M. Calderini, A. Canteaut, C. Carlet, P. Charpin, J. F. Dillon, H. Dobbertin, Y. Edel,

X.-D. Hou, F. Göloğlu, G. Kyureghyan, L. R. Knudsen, G. Leander, G. McGuire, K. Nyberg, A. Pott, S. Yoshiara и др. Несмотря на то, что класс APN-функций активно изучается, в данной области по-прежнему большое количество открытых вопросов.

Например, неизвестно точное число APN-функций, нижние и верхние оценки числа APN-функций, оценка их алгебраической степени. Не так многочисленны и известные конструкции APN-функций — мономиальные функции и несколько полиномиальных, поэтому один из главных вопросов — это существование комбинаторных или итеративных конструкций APN-функций. В частности, интересен вопрос о конструкции APN-функции с помощью композиции или суммы двух функций. Лишь частично описана группа автоморфизмов класса APN-функций и APN-перестановок. В общем случае неизвестно, какими свойствами обладают подфункции APN-функций и существует ли характеризация APN-функции через ее координатные булевы функции.

Один из самых важных открытых вопросов в области APN-функций посвящен проблеме существования взаимно однозначных APN-функций, или *APN-перестановок*. В работе [53] С.-Д. Хоу была выдвинута гипотеза (и доказана для случая $n = 4$ с помощью компьютерных вычислений), что не существует APN-перестановок от четного числа переменных. Однако, в 2009 Дж. Ф. Диллоном и др. (см. [23]) был найден первый пример взаимно однозначной APN-функции от 6 переменных. В работах [31] А. Канто и др., [73] Л. Перрина и др. рассматривается бесконечное семейство векторных функций таких, что $\Delta_F \leqslant 4$, также содержащее APN-функцию Диллона, однако доказано, что это единственная APN-перестановка в данном семействе. До сих пор неизвестно, существуют ли другие APN-перестановки от 6 переменных (неэквивалентные функции Диллона) и существуют ли они вообще для других четных $n > 6$.

Вычисления, возникающие в процессе реализации криптографических алгоритмов, обладают некоторыми специфическими параметрами, такими, как время выполнения операций, электромагнитное излучение или потребляемая мощность. Криптоанализ по сторонним каналам использует эти параметры для того, чтобы восстановить секретную информацию, в частности, закрытый ключ, используемый в шифровании. Одна из самых распространенных техник данного класса криптографических атак — разностная атака по мощности (differential power attack — DPA). Этот вид криптоанализа исследует корреляцию между потребляемой мощностью и промежуточными вычислениями алгоритма.

Методы противодействия атакам по сторонним каналам активно исследуются и разрабатываются в последние несколько лет. Некоторые из них вносят измене-

ния в исследуемые криптоаналитиком параметры, например, добавляют временные задержки в расписание вычислений или вставляют в алгоритм дополнительные операции. Также известны [78] подходы, которые сглаживают разницу в потребляемой мощности для различных промежуточных данных. Альтернативным способом внести некоторую случайность в вычисления является так называемое маскирование. Данный подход может быть реализован как в самом алгоритме [6], [17], [49], [70], [71], так и в дизайне аппаратного устройства [75], [54]. Одним из самых перспективных способов маскирования блочного шифра является метод пороговой реализации, который представляет собой специальное равномерное разбиение S-блоков.

Целью работы является получение новых комбинаторных свойств почти совершенно нелинейных векторных функций и разработка методов построения взаимно однозначных представителей данного класса функций, а также поиск специального разбиения векторных функций, позволяющего противодействовать атакам по сторонним каналам.

Полученные результаты. В работе предложены два метода построения взаимно однозначных APN-функций. Первый из них осуществляет поиск APN-перестановок с помощью EA-эквивалентных 2-в-1 APN-функций. Вводится аппарат символьных последовательностей специального вида — допустимых последовательностей, с помощью которого могут быть получены данные функции, а также описывается способ построения таких последовательностей. С помощью данного метода получены все существующие взаимно однозначные APN-функции от 5 переменных, а также единственная известная APN-перестановка от 6 переменных. Второй метод позволяет искать взаимно однозначные APN-функции $S = (s_1, \ldots, s_n)$ через $(n-1)$-подфункции $(s_1, \ldots, s_{n-1})$, также получаемые с помощью допустимых последовательностей, и недостающие координатные булевы функции s_n. Для произвольной 2-в-1 векторной функции S из специального класса, представимой в виде $S = (s_1, \ldots, s_{n-1})$, получена нижняя оценка числа таких булевых функций s_n, что взаимно однозначная функция $S = (s_1, \ldots, s_n)$ является APN-функцией.

Доказано, что не существует симметрических APN-функций, а также найдены оценки числа симметрических представителей среди их координатных функций. Получена нижняя оценка числа различных значений произвольной APN-функции. Найдена верхняя оценка количества одинаковых значений у произвольной APN-функции.

Предложена оптимизация поиска равномерного разбиения векторных функций, используемого в методе пороговой реализации. С ее помощью доказано,

что не существует равномерного разбиения на 3 части для одного из классов аффинной эквивалентности S-блоков 3×3. Предложен способ пороговой реализации в виде композиции равномерных разбиений.

Данная работа имеет следующую структуру.

Первая глава является обзором имеющихся результатов по проблеме существования взаимно однозначных APN-функций. Описаны известные свойства и характеризации APN-перестановок, а также свойства их компонентных функций и производных. Приведены существующие конструкции взаимно однозначных APN-функций, включая единственную известную на данный момент APN-перестановку от четного числа переменных, а также обобщения данных конструкций. Кроме того, рассматриваются вопросы представления взаимно однозначных APN-функций в виде композиции функций с более простыми свойствами.

Во **второй главе** описывается новый метод поиска взаимно однозначных APN-функций с помощью 2-в-1 APN-функций, которые EA-эквивалентны перестановкам.

Теорема 1. Для любой 2-в-1 векторной функции F от n переменных существует векторная функция G от n переменных, каждая координатная булева функция которой сбалансирована или тождественно равна константе, такая, что функция $H = F + G$ — взаимно однозначна.

Данная теорема влечет за собой следующее: если 2-в-1 функция F — APN-функция, а функция G из условия теоремы является аффинной, то $F + G$ — APN-перестановка, поскольку полученная функция EA-эквивалентна исходной. Это позволяет предложить метод поиска новых APN-перестановок с помощью 2-в-1 APN-функций. Данный метод можно условно разбить на три этапа. На первом этапе строятся всевозможные символьные последовательности, потенциально представляющие собой вектор значений некоторой 2-в-1 APN-функции — *допустимые* последовательности. На следующем этапе символам в построенных последовательностях сопоставляются двоичные векторы, удовлетворяющие специальным ограничениям, в результате чего получаются 2-в-1 APN-функции. На последнем этапе для каждой построенной 2-в-1 APN-функции F мы ищем аффинную функцию, если таковая существует, которая в сумме с F дает APN-перестановку. Также в главе найдены примеры 2-в-1 APN-функций от 5 и 6 переменных, которые EA-эквивалентны APN-перестановкам.

В **третьей главе** вводится понятие $(n-1)$-подфункций APN-перестановок. Показано, что им можно сопоставить дифференциально 4-равномерные 2-в-1 векторные функции, которые могут быть получены методом из предыдущей гла-

вы. Соответственно, с помощью таких 2-в-1 функций возможен поиск новых взаимно однозначных APN-функций.

Напомним, что векторному пространству $\mathbb{F}_2^n$ можно поставить во взаимно однозначное соответствие целочисленное множество $\{0, \ldots, 2^n - 1\}$, где каждое число соответствует двоичному вектору из $\mathbb{F}_2^n$. Рассмотрим 2-в-1 функцию из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$, которая принимает значения исключительно из множества $\{0, \ldots, 2^{n-1}-1\}$, обозначим множество таких 2-в-1 функций от n переменных через $\mathcal{T}_n$. Нетрудно заметить, что любая $(n-1)$-подфункция взаимно однозначной векторной функции есть в точности функция из $\mathcal{T}_n$. Доказаны следующие утверждения.

Теорема 2. Пусть F — взаимно однозначная APN-функция от n переменных. Тогда любая ее $(n-1)$-подфункция является дифференциально 4-равномерной функцией из $\mathcal{T}_n$.

Теорема 3. Пусть F — взаимно однозначная APN-функция от n переменных. Тогда символьная последовательность, соответствующая вектору значений любой ее $(n-1)$-подфункции, является допустимой последовательностью.

Из данных теорем следует, что любая APN-перестановка может быть получена из 2-в-1 дифференциально 4-равномерной функции, построенной при помощи допустимой последовательности. Предложен следующий метод построения взаимно однозначных APN-функций. На первом шаге строятся допустимые символьные последовательности, и для каждой последовательности находится означивание, такое, что полученная 2-в-1 функция является дифференциально 4-равномерной. Следовательно, данной функции соответствует $(n-1)$-подфункция $S = (s_1, \ldots, s_{n-1})$ некоторой взаимно однозначной векторной функции, которая может быть APN-функцией. Это означает, что данная $(n-1)$-подфункция S может быть достроена до APN-перестановки. Для того, чтобы получить эту перестановку, нужно добавить к подфункции S недостающую координатную булеву функцию s_n от n переменных, удовлетворяющую некоторым свойствам. Показано, что существует $2^{2^{n-1}}$ булевых функций s_n таких, что $S = (s_1, \ldots, s_{n-1}, s_n)$ является взаимно однозначной функцией. Однако, для $n \geqslant 7$ данное число слишком велико, поэтому, для того, чтобы оценить эффективность перебора, необходимо найти количество тех булевых функций, которые дают именно APN-перестановку.

Для произвольной взаимно однозначной функции F от n переменных вводится понятие ассоциированной перестановки $F^\star$ от n переменных, необходимое для получения оценки.

Теорема 4. Перестановка F от n переменных является APN-функцией тогда и только тогда, когда перестановка $F^\star$ является APN-функцией.

Пусть S является 2-в-1 дифференциально 4-равномерной функцией из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$, принимающей значения из множества $\{0, \ldots, 2^{n-1}-1\}$, которая может быть представлена в виде $(n-1)$-подфункции $S = (s_1, \ldots, s_{n-1})$. Обозначим через $n(S)$ число таких булевых функций f от n переменных, что $H = (s_1, \ldots, s_{n-1}, f)$ является APN-перестановкой. Получена следующая оценка.

Теорема 5. Если значение $n(S)$ не равно нулю, то $n(S) \geqslant 2^n$.

Четвертая глава посвящена симметрическим свойствам APN-функций, а также структуре и свойствам множества значений произвольной APN-функции.

Напомним определение симметрической функции в двоичном случае. Булева функция от n переменных f — *симметрическая*, если для любой перестановки $\pi \in S_n$ для любых $x_1, \ldots, x_n$ выполнено $f(x_1, \ldots, x_n) = f(x_{\pi(1)}, \ldots, x_{\pi(n)})$. Следующая теорема доказывает невозможность существования APN-функции, сохраняющей свои значения при произвольной перестановке переменных.

Теорема 6. Пусть F — APN-функция от n переменных. Тогда не существует перестановки $\pi \in S_n$, отличной от тождественной, такой что $F(x) = F(\pi(x))$ для любого $x \in \mathbb{F}_2^n$.

Получена следующая верхняя оценка числа координатных симметрических функций APN-функции.

Теорема 7. Пусть F — APN-функция из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$, $F = (f_1, \ldots, f_n)$, где f_i — координатные булевы функции. Тогда, среди $f_1, \ldots, f_n$ не более $\lfloor n - \log_2 C_n^{\lfloor \frac{n-1}{2} \rfloor} \rfloor$ симметрических.

Булева функция называется *инвариантной относительно циклического сдвига (rotation symmetric Boolean function* или *RotS*, см. [74]), если $f(x_1, x_2, \ldots, x_n) = f(x_2, \ldots, x_n, x_1) = \ldots = f(x_n, x_1, \ldots, x_{n-1})$ для любого вектора x. Получена оценка числа координатных функций, инвариантных относительно циклического сдвига.

Теорема 8. Пусть F — APN-функция от n переменных, $F = (f_1, \ldots, f_n)$, где f_i — координатные булевы функции. Тогда, среди $f_1, \ldots, f_n$ не более $\lfloor n - \log_2 n \rfloor$ RotS-функций.

Вторая часть главы 4 посвящена исследованию множества значений произвольной APN-функции. Пусть векторная функция F от n переменных принимает t различных значений $y_1, \ldots, y_t$. Определим множество $M_i = \{x \in \mathbb{F}_2^n \mid F(x) = y_i\}$, где $i = 1, \ldots, t$. Через M_{max} будем обозначать максимальное по мощности множество M_i.

Теорема 9 Пусть F — произвольная APN-функция от n переменных. Тогда выполняется $|M_{max}| \leqslant \sqrt{2^{n+1}-1}+1$.

Также данная оценка улучшена для $n \leqslant 6$.

Теорема 10. Пусть F — APN-функция от n переменных, $n \leqslant 6$. Тогда мощность $|M_{max}|$ не превышает числа $\xi(n)$, где $\xi(n)$ принимает следующие значения:

n	2	3	4	5	6
$\xi(n)$	3	4	6	7	11

Данная оценка является точной.

В **пятой главе** рассматривается метод разбиения S-блоков для защиты от атак по сторонним каналам. Многие криптографические алгоритмы уязвимы к атакам по сторонним каналам, направленным на слабости в практической реализации алгоритма. В качестве мер противодействия используются методы, маскирующие входные данные так, чтобы вычисления не зависели от них в явном виде. В работе [13] описан один из таких методов — пороговая реализация S-блоков.

Рассмотрим векторную функцию $S = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$, где переменная x_i принимает значения из $\mathbb{F}_2$. Для некоторого натурального r представим каждую переменную x_i в виде суммы r новых булевых переменных $x_{i_1}, \ldots, x_{i_r}$, где первые $r-1$ переменных независимы и выбираются случайным образом, а переменная x_{i_r} подбирается так, что справедливо:

$$x_i = \sum_{j=1}^{r} x_{ij}.$$

Пусть $v = (x_{11}, \ldots, x_{nr})$. Представим функцию S в виде суммы r векторных функций:

$$S(x) = \sum_{j=1}^{r} S_j(v),$$

где $S_i : \mathbb{F}_2^{nr} \to \mathbb{F}_2^n$. Набор из r векторных функций $S_1, \ldots, S_r$ называется *разбиением* S-блока S *на* r *частей*. Введем следующие условия для разбиения:

1. *Неполнота*: для каждого $j = 1, \ldots, r$ функция S_j не должна зависеть от переменных x_{ij}, $i = 1, \ldots, n$.

2. *Взаимная однозначность*: функция $S^* : \mathbb{F}_2^{nr} \to \mathbb{F}_2^{nr}$, где $S^* = (S_1, \ldots, S_r)$ является взаимно однозначной.

Разбиение, удовлетворяющее этим двум условиям, называется *равномерным* разбиением.

Отношение аффинной эквивалентности разбивает множество всех взаимно однозначных S-блоков на непересекающиеся классы. Множество S-блоков 3×3 содержит 4 класса, $\mathcal{A}_1^3$, $\mathcal{Q}_1^3$, $\mathcal{Q}_2^3$, $\mathcal{Q}_3^3$ (см. [16]).

Класс	Представитель	Вектор значений
$\mathcal{A}_1^3$	(x, y, z)	$(0\ 1\ 2\ 3\ 4\ 5\ 6\ 7)$
$\mathcal{Q}_1^3$	$(x, y, xy + z)$	$(0\ 1\ 2\ 3\ 4\ 5\ 7\ 6)$
$\mathcal{Q}_2^3$	$(x, y + xz, z + xy + xz)$	$(0\ 1\ 2\ 3\ 4\ 6\ 7\ 5)$
$\mathcal{Q}_3^3$	$(xy + xz + yz, x + y + xy + yz, x + z + yz)$	$(0\ 1\ 2\ 4\ 3\ 6\ 7\ 5)$

Для всех классов, кроме $\mathcal{Q}_3^3$, ранее в [13] было найдено равномерное разбиение. Однако большой перебор не позволил найти для класса $\mathcal{Q}_3^3$ соответствующее разбиение или доказать, что его не существует.

В данной главе предложен способ (см. Теорему 11) оптимизации поиска равномерного порогового разбиения для S-блока от произвольного числа переменных. С помощью компьютерных вычислений получен следующий результат.

Утверждение 9. Для S-блоков из класса $\mathcal{Q}_3^3$ не существует равномерного разбиения на 3 части.

Ввиду несуществования равномерного порогового разбиения для данного класса, предложен метод реализации S-блоков из $\mathcal{Q}_3^3$ в виде композиции двух S-блоков, для каждого из которых уже существует требуемое пороговое разбиение.

Научная новизна и значимость. Вопрос существования взаимно однозначных APN-функций от четного числа переменных является центральным (см. [35]) открытым вопросом в области векторных булевых функций. Напомним, что уже при $n = 6$ про класс APN-функций практически ничего неизвестно — классификация APN-функция получена (см. [21]) только при $n \leqslant 5$, причем удалось ее осуществить лишь в результате масштабной теоретической оптимизации вычислений.

Впервые данная проблема была упомянута в 1998 году в статье [36] К. Карле, П. Шарпин и В. Зиновьева и явным образом сформулирована через год в работе [41] Х. Доббертина. Долгое время считалось, что не существует взаимно однозначных APN-функций для четных n. Данная гипотеза была вычислительно доказана для $n = 4$ в работе [53] С.-Д. Хоу. Лишь в 2017 году появилось [29] первое теоретическое доказательство того, что не существует APN-перестановок от 4 переменных. Заметим, что ввиду Теоремы 2 любая $(n-1)$-подфункция APN-перестановки является дифференциально 4-равномерной функцией из $\mathcal{T}_n$. В данной работе получено, что в $\mathcal{T}_4$ не существует дифференциально 4-равномерных

функций, таким образом, этот факт также является доказательством того, что не существует APN-перестановок от 4 переменных.

Первый пример взаимно однозначной APN-функции от 6 переменных был найден лишь в 2009 Дж. Ф. Диллоном и др. (см. [23]). Эта APN-перестановка является единственной (с точностью до эквивалентности) известной на данный момент взаимно однозначной APN-функцией от четного числа переменных. Полученная APN-перестановка сразу же нашла применение в качестве S-блока в легковесном шифре FIDES. APN-функция Диллона была получена при помощи аппарата теории кодирования из CCZ-эквивалентной APN-функции над конечным полем, которая не являлась взаимно однозначной. Данный подход не использовал непосредственных конструкций, ни комбинаторных, ни над конечным полем. Семейство взаимно однозначных функций, исследованное через несколько лет в работах [73] и [31] и содержащее APN-функцию Диллона, было построено уже с помощью некоторой конструкции над конечным полем. Кроме того, в работах [57]и [59] были найдены APN-перестановки от 6 переменных (CCZ-эквивалентные APN-функции Диллона), которые также были получены через конструкции над конечным полем со специальными условиями на коэффициенты. Однако, ни для APN-функции Диллона, ни для взаимно однозначных APN-функций от нечетного числа переменных до сих пор не существовало ни одной комбинаторной конструкции, и, более того, комбинаторный подход никогда не применялся к проблеме существования APN-перестановок.

Данная работа предлагает два комбинаторных метода (Метод 2 и Метод 3) построения взаимно однозначных APN-функций для любого n — как четного, так и нечетного. Метод 2 строит APN-перестановки через сумму 2-в-1 APN-функций и аффинных векторных функций, а Метод 3 использует дифференциально 4-равномерные функции вида $S = (s_1, \ldots, s_{n-1})$, которые достраиваются до APN-перестановки $S = (s_1, \ldots, s_n)$ добавлением недостающих координатных булевых функций s_n. Доказано, что любая взаимно однозначная APN-функция может быть построена с помощью Метода 3. Кроме того, в данной работе показано (см. Таблицу 2.3), что APN-функция Диллона может быть построена с помощью Метода 2, как и все существующие APN-перестановки от 5 переменных (см. Таблицу 2.2).

Помимо того, что в $\mathcal{T}_4$ не существует дифференциально 4-равномерных функций, в работе также показано, что не существует 2-в-1 APN-функций от 4 переменных, в то время как для 6 переменных оба класса функций уже существуют. Вместе с другими теоретическими результатами, полученными в данной работе, этот факт позволяет предполагать, что проблема существования взаимно одно-

значных APN-функций может быть сведена к существованию дифференциально 4-равномерных функций, принимающих значения из $\{0, \ldots, 2^{n-1} - 1\}$, а также к существованию 2-в-1 APN-функций, для построения которых в работе предложен Метод 1.

Напомним, что взаимно однозначная векторная функция от 8 переменных, используемая в шифре AES — стандарте шифрования США, является лишь дифференциально 4-равномерной функцией. Поэтому, если будет найдена APN-перестановка от 8 переменных, она может заменить собой имеющийся S-блок шифра.

Класс преобразований, сохраняющий свойство функции быть APN-перестановкой не описан полностью — известно лишь, что функция, аффинно эквивалентная взаимно однозначной APN-функции, также является APN-перестановкой. В работе предложено конструктивное определение ассоциированной перестановки и доказано, что перестановка F от n переменных является APN-функцией тогда и только тогда, когда любая ее ассоциированная перестановка $F^\star$ является APN-функцией. Это определение описывает новое преобразование, которое является автоморфизмом класса взаимно однозначных APN-функций.

Интуитивно понятно, что множество значений произвольной APN-функций должно быть довольно разнообразным, но данный вопрос никогда не исследовался и структура вектора значений APN-функции ранее не рассматривалась. В работе получена нижняя оценка числа различных значений произвольной APN-функций, а также верхняя оценка числа ее одинаковых значений, кроме того, эта оценка улучшена для $n \leqslant 6$. Данные результаты могут быть использованы для дальнейшей классификации APN-функций (напомним, что классификация получена лишь для $n \leqslant 5$), поскольку они существенно ограничивают пространство перебора векторных функций.

Предложенный в [62] метод пороговой реализации S-блоков показал свою эффективность для защиты шифра от атак по сторонним каналам. Однако, ввиду большого числа возможных разбиений (которое составляет 2^{54}) для S-блоков всего лишь от трёх переменных уже не представлялось возможным осуществить полный перебор, чтобы найти требуемое равномерное разбиение для одного из классов эквивалентности S-блоков или доказать, что его не существует. Несколько лет этот вопрос оставался открытым [13], пока в данной работе не удалось получить теоретический результат (см. Теорему 11), который позволил значительно сократить перебор и осуществить поиск. Полученный результат справедлив для S-блоков от любого числа переменных, поэтому данная оптимизация

может быть использована для поиска равномерного разбиения и в других размерностях.

Публикации. Основные результаты по теме диссертации изложены в 13 печатных изданиях [78 — 90], 4 из которых изданы в журналах, рекомендованных ВАК [78 — 81], 9 — в тезисах и трудах конференций [82 — 90].

Апробация работы. Основные результаты работы докладывались на следующих конференциях и семинарах: Международной конференции «Boolean Functions and their Applications (BFA)» (2017, г. Ос, Норвегия, 2018, г. Луэн, Норвегия), Сибирской научной школе-семинаре с международным участием «Компьютерная безопасность и криптография» (SIBECRYPT, 2012 — 2016), семинаре лаборатории компьютерной безопасности и криптографии COSIC (г. Левен, Бельгия, 2013), семинаре исследовательского центра безопасности коммуникаций им. Э. С. Селмера (г. Берген, Норвегия, 2016), Мальцевских чтениях в 2013 году в Новосибирске, семинарах «Дискретный анализ» и «Криптография и криптоанализ» Института математики им. С. Л. Соболева и кафедры теоретической кибернетики НГУ, семинаре отдела теоретической кибернетики ИМ СО РАН.

Благодарности. Я выражаю глубокую признательность своему научному руководителю Наталье Николаевне Токаревой за постоянное внимание к моей работе и неоценимую всестороннюю помощь на протяжении моего научного пути. Я очень благодарна своему мужу Идрисову Ренату Искандеровичу за консультации в вопросах написания программ, за помощь в проведении вычислений и за беспрестанную поддержку во время написания данной работы. Также я признательна рецензентам своих статей за ценные замечания, дополнения и предложения, которые значительно улучшили качество моих печатных работ. Приношу свою благодарность Александру Андреевичу Евдокимову, членам лаборатории дискретного анализа и другим сотрудникам Института математики им. С. Л. Соболева СО РАН за постоянную поддержку и интерес к моему труду. Я выражаю искреннюю благодарность Лилии Будагян и Марко Калдерини из университета г. Бергена за консультации по вопросам APN-функций и за помощь в доказательстве одной из гипотез. Отдельно хотелось бы выразить признательность своим коллегам Анастасии Городиловой и Николаю Коломейцу за плодотворную совместную работу, содержательные дискуссии и помощь в любых вопросах.

Глава 1

Взаимно однозначные APN-функции. Обзор известных результатов

Впервые проблема существования взаимно однозначных APN-функций при четном n была упомянута в статье [36] и явно сформулирована в работе [41]. Первоначально считалось [53], что не существует APN-перестановок от четного числа переменных, и данная гипотеза была доказана для случая $n = 4$. Однако, в 2009 году в работе [23] была найдена первая взаимно однозначная APN-функция от 6 переменных. Несмотря на многочисленные исследования, посвященные APN-функциям, про взаимно однозначных представителей данного класса известно по-прежнему не так много. Данная глава посвящена известным результатам в области конструкций, свойств и характеризаций APN-перестановок.

1.1 Характеризации и свойства взаимно однозначных APN-функций

1.1.1 Свойства координатных и компонентных булевых функций у взаимно однозначных APN-функций

Для компонентных булевых функций взаимно однозначных векторных функций известен следующий результат.

Предложение 1. *(см. [34], [58]) Векторная функция F из $\mathbb{F}_2^n$ в $\mathbb{F}_2^m$ уравновешена тогда и только тогда, когда любая ее компонентная функция сбалансирована.*

Следующее общее свойство координатных функций APN-функций справедливо для взаимно однозначных представителей.

Предложение 2. *(см. [9]) Пусть $F = (f_1, \ldots, f_n)$ — взаимно однозначная APN-функция от n переменных. Тогда ни одна координатная булева функция из $f_1, \ldots, f_n$ не является аффинной.*

Одним из главных открытых вопросов в области APN-функций является вопрос существования комбинаторных конструкций (напомним, что все имеющиеся конструкции являются конструкциями над конечным полем), в частности, вопрос — какими свойствами обладает алгебраическая нормальная форма APN-функции? Один из немногих известных результатов по этому вопросу формулируется следующим образом.

Предложение 3. *(см. [9]) Пусть $F = (f_1, \ldots, f_n)$ — взаимно однозначная APN-функция от n переменных. Тогда каждый из возможных двучленов $x_i x_j$, где $(i \neq j)$, встретится в алгебраической нормальной форме хотя бы одной из координатных функций $f_1, \ldots, f_n$.*

Известно [9], что максимальная алгебраическая степень взаимно однозначной функции от n переменных равна $n-1$, что справедливо и для APN-перестановок. Интересно, однако, что и для произвольной APN-функции это, скорее всего, справедливо. Так, в работе [28] выдвинута и частично доказана гипотеза о том, что не существует APN-функций от n переменных алгебраической степени n, если $n \geqslant 3$.

Напомним, что для произвольного ненулевого вектора $\lambda \in \mathbb{F}_2^m$ линейная комбинация координатных функций $f_\lambda = \lambda \cdot F$ называется *компонентной функцией*. Пусть f — булева функция от n переменных. Обозначим через $\mathcal{F}(f)$ следующую величину:

$$\mathcal{F}(f) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)} = 2^n - 2wt(f),$$

где $wt(f)$ — вес Хэмминга данной функции.

В работе [7] показано, что существует полная характеризация взаимно однозначных APN-функций через производные их компонентных булевых функций.

Предложение 4. *(см. [7]) Пусть F — векторная функция из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$ с компонентными функциями f_λ, $\lambda \in \mathbb{F}_2^n$. Тогда F является взаимно однозначной APN-функцией тогда и только тогда, когда для любого ненулевого $a \in \mathbb{F}_2^n$ выполнены следующие условия:*

$$\sum_{\lambda \in \mathbb{F}_2^n, \lambda \neq 0} \mathcal{F}(D_a(f_\lambda)) = -2^n$$

и

$$\sum_{\lambda \in \mathbb{F}_2^n, \lambda \neq 0} \mathcal{F}^2(D_a(f_\lambda)) = 2^{2n}.$$

Пусть $D_1(f)$ — производная функции f по направлению вектора, состоящего из всех единиц. В случае нечетного n для мономиальных функций справедлива следующая характеризация.

Предложение 5. *(см. [7]) Пусть F — векторная функция над полем $\mathbb{F}_{2^n}$ вида $x \mapsto x^d$ и $gcd(d, 2^n - 1) = 1$. Тогда F является взаимно однозначной APN-функцией тогда и только тогда, когда $\sum_{\lambda \in \mathbb{F}_2^n} \mathcal{F}^2(D_1(f_\lambda)) = 2^{2n+1}$.*

Для производных компонентных функций справедливо следующее утверждение.

Предложение 6. *(см. [29]) Пусть F — взаимно однозначная APN-функция от n переменных, где n — четное. Если существуют такие $a, \lambda \in \mathbb{F}_2^n$, что функция $D_a(f_\lambda)$ тождественна равна константе, то $D_a(f_\lambda) = 1$.*

Булева функция f называется *платовидной*, если для некоторого целого c выполняется $W_f(a) \in \{0, \pm 2^c\}$ для любого вектора $a \in \mathbb{F}_2^n$. Следующее утверждение показывает, что не существует таких APN-перестановок, что все их компонентные функции платовидны.

Предложение 7. *(см. [7]) Пусть n — четное, F — APN-функция из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$ и все компонентные функции f_λ, $\lambda \in \mathbb{F}_2^n$ являются платовидными. Тогда F — не взаимно однозначная функция. Более того, не существует такой линейной функции L, что $F + L$ — взаимно однозначная функция.*

Напомним, что *бент-функцией* называется булева функция от четного числа переменных, чьи коэффициенты Уолша-Адамара равны $\pm 2^{n/2}$. Булева функция f называется *частично бент-функцией* [33], если существуют два подпространства U и V, такие, что $U \oplus V = \mathbb{F}_2^n$ и функция f на пространстве U является бент-функцией, а на пространстве V — аффинной. В работе [67] получен следующий результат.

Предложение 8. *(см. [67]) Пусть F — взаимно однозначная функция от n переменных, где n — четное, и все ее компонентные функции частично бент. Тогда F не является APN-функцией. В частности, не существует квадратичных взаимно однозначных APN-функций из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$.*

Известно [79], что каждая частично бент-функция является платовидной. В работе [7] доказано обобщение Предложения 8 на случай платовидных компонентных функций.

Предложение 9. *(см. [7]) Пусть n — четное, F — взаимно однозначная функция из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$, и все компонентные функции f_λ, $\lambda \in \mathbb{F}_2^n$, являются платовидными. Тогда F не является APN-функцией.*

В работе [29] Предложение 8 было усилено.

Предложение 10. *(см. [29]) Пусть n — четное, F — взаимно однозначная APN-функция из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$. Тогда любая компонентная функция векторной функции F не является частично бент-функцией.*

Заметим, однако, что среди компонентных функций APN-перестановок от четного числа переменных могут быть платовидные. Так, например, APN-функция Диллона имеет платовидные компонентные функции. Известно [29], что если векторная функция имеет компонентные функции, являющиеся частично бент-функциями, то любая EA-эквивалентная ей функция также имеет такие компонентные функции.

Предложение 11. *(см. [29]) Пусть n — четное, F — APN-функция из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$. Пусть среди компонентных функций F найдется частично бент-функция или квадратичная функция. Тогда не существует перестановки, которая EA-эквивалентна функции F.*

1.2 Конструкции взаимно однозначных APN-функций

Как уже упоминалось ранее, проблема существования взаимно однозначных APN-функций актуальна только для четного случая. Для нечетных размерностей существует несколько алгебраических конструкций APN-перестановок над конечным полем. Так, в 1998 году Х. Доббертином доказано следующее утверждение.

Предложение 12. *(см. [43]) Мономиальные APN-функции из таблицы 1 при нечетном n являются взаимно однозначными.*

Путем компьютерных вычислений было доказано [53], что при $n = 4$ взаимно однозначных APN-функций не существует. Однако, никаких теоретических доказательств данного факта до недавнего времени не существовало. В работе [29] доказан следующий факт.

Предложение 13. *(см. [29]) Пусть F — векторная функция от 4 переменных и все её ненулевые компонентные функции имеют степень 3. Тогда F не является APN-функцией.*

Авторами [29] показано, что у всех взаимно однозначных векторных функций от 4 переменных компонентные функции являются кубическими. Отсюда следует, что для размерности 4 взаимно однозначных APN-функций не существует.

1.2.1 Взаимно однозначные APN-функции от четного числа переменных. Функция Диллона

В работе [23] авторы рассматривали APN-функцию Кима $\kappa(x) = x^3 + x^{10} + ux^{24}$, где u — примитивный элемент поля $GF(2^6)$, а поле $GF(2^6)$ построено с помощью многочлена $x^6+x^4+x^3+x+1$. Используя аппарат теории кодирования и представляя отношение CCZ-эквивалентности в специальном матричном виде, авторам удалось доказать следующее утверждение.

Предложение 14. *(см. [23]) Функция $\kappa(x)$ является CCZ-эквивалентной взаимно однозначной APN-функции.*

Первый пример взаимно однозначной APN-функции (т.н. функции Диллона) от 6 переменных, найденный в работе [23], имеет следующий вектор значений (см. Таблицу 1.1).

Таблица 1.1: APN-функция Диллона.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	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	58	59	60	61	62	63
$F(x)$	0	54	48	13	15	18	53	35	25	63	45	52	3	20	41	33
	59	36	2	34	10	8	57	37	60	19	42	14	50	26	58	24
	39	27	21	17	16	29	1	62	47	40	51	56	7	43	44	38
	31	11	4	28	61	46	5	49	9	6	23	32	30	12	55	22

Алгебраическая степень найденной взаимно однозначной функции равна 4. Функция Диллона имеет следующее представление над конечным полем:

$G(x) = w^{45}x^{60} + w^{41}x^{58} + w^{43}x^{57} + w^{4}x^{56} + w^{50}x^{54} + w^{20}x^{53} + w^{45}x^{52} + w^{20}x^{51} + w^{23}x^{50} + w^{36}x^{49} + w^{56}x^{48} + w^{21}x^{46} + w^{5}x^{45} + w^{21}x^{44} + w^{28}x^{43} + w^{3}x^{42} + w^{59}x^{41} +$

$w^{58}x^{40} + w^{57}x^{39} + w^{53}x^{38} + w^{37}x^{37} + w^{40}x^{36} + w^{18}x^{35} + w^{41}x^{34} + w^{54}x^{33} + w^{3}x^{32} + w^{49}x^{30} + w^{41}x^{29} + w^{42}x^{28} + w^{50}x^{27} + w^{53}x^{26} + w^{58}x^{25} + w^{9}x^{24} + x^{23} + w^{28}x^{22} + w^{3}x^{21} + w^{21}x^{20} + w^{52}x^{19} + w^{60}x^{17} + w^{59}x^{16} + w^{10}x^{15} + w^{42}x^{13} + w^{8}x^{12} + w^{35}x^{11} + w^{44}x^{10} + w^{45}x^{8} + w^{8}x^{7} + w^{61}x^{6} + w^{59}x^{5} + w^{20}x^{4} + w^{12}x^{3} + w^{37}x^{2} + w^{2}x,$

где $w = u^{-2}$. Функция G получена как композиция следующих векторных функций:

$$G := F_2 \circ F_1^{-1}$$

где функция F_1 имеет следующее представление над полем:

$F_1(x) = w^{38}x^{48} + w^{33}x^{40} + w^{28}x^{34} + w^{25}x^{33} + w^{43}x^{32} + w^{5}x^{24} + w^{42}x^{20} + x^{17} + w^{2}x^{16} + w^{4}x^{12} + w^{7}x^{10} + w^{58}x^{8} + w^{59}x^{6} + w^{5}x^{5} + w^{36}x^{4} + w^{47}x^{3} + w^{30}x^{2} + w^{9}x,$

а функция F_2 имеет представление:

$F_2(x) = w^{26}x^{48} + w^{60}x^{40} + w^{46}x^{34} + w^{6}x^{33} + w^{61}x^{32} + w^{51}x^{24} + w^{53}x^{20} + w^{61}x^{17} + w^{54}x^{16} + w^{55}x^{12} + w^{33}x^{10} + w^{33}x^{8} + w^{19}x^{6} + w^{46}x^{5} + w^{51}x^{4} + w^{16}x^{3} + w^{37}x^{2} + w^{27}x.$

Заметим, что функции F_1 и F_2 имеют алгебраическую степень 2, функция F_1^{-1} имеет алгебраическую степень 3.

Полученная Диллоном APN-функция сразу же нашла применение, в частности, в качестве S-блока в аутентификационном шифре FIDES (см. [12]).

1.2.2 Обобщения функции Диллона

В работе [73] метод обратного инжиниринга, который позволяет провести глубокий анализ структуры S-блоков, был применен к APN-функции Диллона. Авторами было получено более простое и компактное представление данной функции в виде специальной структуры, состоящей из двух перестановок над $\mathbb{F}_2^3$ — TU-разложения. Также найдено и описано семейство взаимно однозначных *функций-бабочек*, которое включает в себя исходную APN-функцию.

Это семейство далее исследовалось в работе [31], где было обобщено на случай четных размерностей для $n > 6$, однако, за исключением функции Диллона и эквивалентных ей функций, только дифференциально 4-равномерные представители входят в обобщение семейства. Полученное семейство функций обладает также наилучшей известной нелинейностью $2^{n/2+1}$ для случая $n = 4k+2, k \geqslant 1$.

В работе [57] рассматривалась функция $F(x) = x^3 + Ax^{3\cdot 2^m} + Bx^{2^{m+1}+1} + Cx^{2+2^m}$ над конечным полем $GF(2^m)$, где $A, B, C \in GF(2^m)$. Авторами были получены необходимые и достаточные условия на коэффициенты A, B и C для того, чтобы функция F являлась APN-функцией. Были найдены 112 APN-функций, имеющих данное полиномиальное представление, 84 из которых являлись APN-перестановками. В работе [59] с помощью аппарата эллиптических кривых так-

же были найдены взаимно однозначные APN-функции от 6 переменных. Однако, все найденные на данный момент APN-перестановки CCZ-эквивалентны APN-функции Диллона.

1.3 Разложение взаимно однозначных APN-функций

При реализации в шифрах зачастую требуется упростить представление S-блоков, например, разложить векторную функцию в виде композиции функций с более простыми свойствами. Так, подробно рассмотренная в предыдущем разделе APN-функция Диллона представима в виде композиции двух взаимно однозначных функций меньших степеней. Для векторной функции F такое представление $F(x) = G_t \circ G_{t-1} \circ \ldots \circ G_1(x)$ называется *декомпозицией*.

В работе [65] был представлен новый метод разложения взаимно однозначных векторных функций функций меньшей степени, в частности, квадратических и кубических функций. Следующее утверждение справедливо также и для взаимно однозначных APN-функций.

Предложение 15. *(см. [65]) Любая взаимно однозначная функция F от n переменных, где $n \leqslant 16$, представима в виде композиции квадратичных взаимно однозначных функций, если n не делится на 4. В случае, когда n делится на 4, функция F представима в виде композиции кубических взаимно однозначных функций.*

Кроме того, для всех (с точностью до аффинной эквивалентности) взаимно однозначных APN-функций от 5 переменных и функции обращения в поле $x \mapsto x^{-1}$ для $n \leqslant 16$ были получены соответствующие декомпозиции.

1.4 Группа автоморфизмов APN-перестановок

Вопрос описания преобразований, сохраняющих криптографические свойства булевых и векторных функций, а также построение соответствующих классов эквивалентности, имеет большую теоретическую и практическую важность, поскольку позволяет решить некоторые фундаментальные задачи в криптографии. Такими, например, являются проблема построения новых функций с заданными свойствами, описание структуры множества функций с заданными характеристиками, поиск функции, наилучшей по параметрам для данного приложения, а тажке вопросы классификации функций.

Напомним, что векторные булевы функции F и G называются *расширенно аффинно эквивалентными (EA-эквивалентными)*, если $F = A_1 \circ G \circ A_2 + A$, где A_1, A_2 — взаимно однозначные аффинные функции над $\mathbb{F}_2^n$ и A — аффинная функция. В случае $A \equiv \mathbf{0}$, функции F и G называются *аффинно эквивалентными*.

Две функции F и G называются *CCZ-эквивалентными*, если соответствующие множества $\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \mid y = F(x)\}$ и $\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \mid y = G(x)\}$ являются аффинно эквивалентными, или, если существует аффинный автоморфизм $A = (A_1, A_2)$ такой, что $y = F(x) \Leftrightarrow A_2(x, y) = G(A_1(x, y))$. Понятие CCZ-эквивалентности неявным образом появилось в статье [36], а потом было формально определено в статье [27]. Оно непосредственным образом связано с кодовым представлением векторной функции. Напомним, что *линейным кодом* с параметрами $[n, k, d]$ называется подпространство векторного пространства $\mathbb{F}_2^n$, где n — длина кодовых слов, k — размерность кода, а d — кодовое расстояние.

Предложение 16. *(см. [36]) Пусть F — векторная функция из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$, $F(\boldsymbol{0}) = \boldsymbol{0}$, а C_F — соответствующий линейный код с параметрами $[2^n - 1, k, d]$, заданный следующей проверочной матрицей:*

$$\mathcal{H}_F = \begin{pmatrix} x_1 & x_2 & x_3 & \dots & x_n \\ F(x_1) & F(x_2) & F(x_2) & \dots & F(x_n) \end{pmatrix}$$

Тогда:
1) выполнено $3 \leqslant d \leqslant 5$;
2) функция F является APN тогда и только тогда, когда $d = 5$.

Отсюда и возникает понятие CCZ-эквивалентности, как эквивалентности соответствующих линейных кодов. Известно, что EA-эквивалентные функции являются в то же время CCZ-эквивалентными, однако, обратное в общем случае неверно.

Предложение 17. *(см. [27]) Если $n \geqslant 5$ и $m > 1$ — любой делитель числа n, или выполнено $n = m = 4$, то для таких векторных (n, m)-функций, CCZ-эквивалентность является строго более общей, чем EA-эквивалентность.*

Известно, что если F из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$ является APN-перестановкой, то любые EA-эквивалентные и CCZ-эквивалентные ей функции являются APN-функциями. Однако, в общем случае свойство взаимной однозначности не сохраняется.

Нетрудно заметить, что если векторные булевы функции F и G являются EA-эквивалентными, причем A — функция, тождественно равная константе, а F — APN-перестановка, то G также является APN-перестановкой.

Результаты, полученные в Главе 3, также определяют отношение эквивалентности на множестве APN-перестановок. Мы выбираем натуральное число k, набор индексов $i_1 < \ldots < i_k$ и разбиваем $\mathbb{F}_2^n$ на два непересекающихся подмножества $\mathcal{F}_1^{i_1,\ldots,i_k}$ и $\mathcal{F}_2^{i_1,\ldots,i_k}$. Далее, для некоторого индекса $j \notin \{i_1, \ldots, i_k\}$ мы определяем ассоциированную перестановку $F^\star$ следующим образом:

$$F^\star(x) = \begin{cases} F(x), & \text{если } F(x) \in \mathcal{F}_1^{i_1,\ldots,i_k}; \\ F(x) + e_j, & \text{если } F(x) \in \mathcal{F}_2^{i_1,\ldots,i_k}. \end{cases}$$

Для данной конструкции в Главе 3 доказана следущая теорема.

Теорема 4. Перестановка F от n переменных является APN-функцией тогда и только тогда, когда ассоциированная перестановка $F^\star$ является APN-функцией.

Теорема 4 задает отношение эквивалентности, однако, неизвестно, как соотносится данная эквивалентность с такими отношениями эквивалентности, как CCZ-эквивалентность и EA-эквивалентность.

Также существует [50] понятие дифференциально эквивалентных векторных булевых функций как функций, имеющих одинаковые ассоциированные булевы функции. В работе [36] для векторной функции F из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$ вводится *ассоциированная булева функция* γ_F от $2n$ переменных, определенная по правилу:

$$\gamma_F(a,b) = \begin{cases} 1, & \text{если } a \neq \mathbf{0} \text{ и уравнение } F(x) \oplus F(x \oplus a) = b \text{ имеет решение;} \\ 0, & \text{иначе.} \end{cases}$$

где $a, b \in \mathbb{F}_2^n$. Известно, что F — APN-функция тогда и только тогда, когда $wt(\gamma_F) = 2^{2n-1} - 2^{n-1}$.

Функции F и G называются *дифференциально эквивалентными*, если $\gamma_F = \gamma_G$. Данное направление еще мало исследовано, однако вопрос дифференциальной эквивалентности APN-перестановок представляет большой интерес для дальнейшего изучения.

Глава 2

Метод построения 2-в-1 APN-функций и проблема существования APN-перестановок

Данная глава посвящена проблеме существования взаимно однозначных функций от четного числа переменных. Предложен метод поиска взаимно однозначных APN-функций через 2-в-1 APN-функции. Доказано, что для любой 2-в-1 векторной функции F существует функция G, каждая координатная булева функция которой сбалансирована или константна, такая, что $F + G$ – взаимно однозначная функция. Из этого факта следует, что среди 2-в-1 функций могут быть EA-эквивалентные перестановкам, поэтому возникает естественный вопрос о том, как строить 2-в-1 APN-функции и с их помощью осуществлять поиск взаимно однозначных APN-функций. Введено понятие допустимой символьной последовательности – последовательности, потенциально представляющей собой вектор значений некоторой 2-в-1 APN-функции. Описан метод построения всевозможных допустимых последовательностей. Далее, символам в построенных последовательностях присваиваются двоичные векторы, удовлетворяющие специальным ограничениям, в результате чего получаются 2-в-1 APN-функции. На заключительном этапе для каждой построенной функции F мы ищем аффинную функцию, которая в сумме с F дает APN-перестановку. Найдены 2-в-1 APN-функции, которые EA-эквивалентны всем APN-перестановкам от 5 переменных и APN-функции Диллона от 6 переменных, а также соответствующие аффинные функции.

2.1 Векторные 2-в-1 функции EA-эквивалентные перестановкам

В данном разделе рассматривается класс 2-в-1 векторных функций и доказывается, что некоторые представители данного класса могут быть EA-эквивалентны взаимно однозначным функциям.

Теорема 1. *Для любой 2-в-1 векторной функции F от n переменных существует векторная функция G, каждая координатная булева функция которой сбалансирована или константна, такая, что $H = F + G$ — взаимно однозначная функция.*

Доказательство. Рассмотрим произвольную 2-в-1 функцию $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Заметим, что ее вектор значений можно разбить на 2^{n-1} пар одинаковых значений. Рассмотрим произвольную пару равных векторов $y_{i_1} = F(x_{i_1})$ и $y_{i_2} = F(x_{i_2})$, а также множество $\{w_1, \ldots, w_{2^n}\}$, состоящее из всех векторов, принадлежащих $\mathbb{F}_2^n$. Без ограничения общности зафиксируем вектор w_{i_1}. Тогда существует вектор z_{i_1} из $\mathbb{F}_2^n$ такой, что $y_{i_1}+z_{i_1} = w_{i_1}$. Положим $z_{i_2} = z_{i_1}+\mathbf{1}$. Тогда $y_{i_2}+z_{i_2} = w_{i_1}+\mathbf{1} = w_{i_2}$. Данный процесс описан на схеме ниже (порядок векторов указан без ограничения общности):

$$\begin{array}{ccccc} F & & G & & H \\ \ldots & & \ldots & & \ldots \\ y_{i_1} & + & z_{i_1} & = & w_{i_1} \\ \ldots & & \ldots & & \ldots \\ y_{i_2} & + & z_{i_2} & = & w_{i_2} \\ \ldots & & \ldots & & \ldots \end{array}$$

Теперь рассмотрим другую пару одинаковых значений функции F, скажем, y_{i_3} и y_{i_4}, а также выберем w_{i_3}, где $i_3 \neq i_1$ и $i_3 \neq i_2$, то есть $w_{i_3} \neq w_{i_1}$ и $w_{i_3} \neq w_{i_2}$. Как и ранее, пусть z_{i_3} — это вектор из $\mathbb{F}_2^n$ такой, что $y_{i_3} + z_{i_3} = w_{i_3}$, и положим $z_{i_4} = z_{i_3}+\mathbf{1}$. Тогда $y_{i_4}+z_{i_4} = w_{i_3}+\mathbf{1} = w_{i_4}$ и $w_{i_4} \neq w_{i_1}, w_{i_2}$, поскольку $w_{i_3} \neq w_{i_1}, w_{i_2}$.

$$
\begin{array}{ccccc}
F & & G & & H \\
\dots & & \dots & & \dots \\
y_{i_1} & + & z_{i_1} & = & w_{i_1} \\
\dots & & \dots & & \dots \\
y_{i_3} & + & z_{i_3} & = & w_{i_3} \\
\dots & & \dots & & \dots \\
y_{i_2} & + & z_{i_2} & = & w_{i_2} \\
\dots & & \dots & & \dots \\
y_{i_4} & + & z_{i_4} & = & w_{i_4} \\
\dots & & \dots & & \dots
\end{array}
$$

Таким образом, повторяя данные шаги, мы получим векторную булеву функцию G такую, что $F+G=H$, где H — взаимно однозначная функция, поскольку все векторы из $\mathbb{F}_2^n$ присутствуют среди ее значений. Рассмотрим функцию G. По построению, для каждого вектора z_{i_k}, встречающегося среди значений функции G, вектор $z_{i_k}+\mathbf{1}$ также будет принадлежать множеству значений функции G. Следовательно, каждая координатная функция векторной функции G является сбалансированной булевой функцией.

Рассмотрим случай, когда, по крайней мере, одна из координатных булевых функций 2-в-1 функции $F=(f_1,\dots,f_n)$ является сбалансированной. Покажем, что в таком случае функция G может иметь координатную функцию, являющуюся константной. Без ограничения общности, пусть f_1 — сбалансированная булева функция. Тогда координатная функция g_1 может быть выбрана как константная функция ($g_1\equiv 0$ или $g_1\equiv 1$), а $g_2,\dots,g_n$ могут быть получены способом выше, однако в этом случае выбор значений w_{i_k}, где $k=1,\dots,2^n$, будет уже не столь гибким, поскольку первая координатная функция H будет зафиксирована как f_1+g_1:

$$
\begin{array}{ccccc}
F & & G & & H \\
\dots & & \dots & & \dots \\
y_{i_1} & + & 0, \overline{z_{i_1}} & = & w_{i_1} \\
\dots & & \dots & & \dots \\
y_{i_3} & + & 0, \overline{z_{i_3}} & = & w_{i_3} \\
\dots & & \dots & & \dots \\
y_{i_2} & + & 0, \overline{z_{i_2}} & = & w_{i_2} \\
\dots & & \dots & & \dots \\
y_{i_4} & + & 0, \overline{z_{i_4}} & = & w_{i_4} \\
\dots & & \dots & & \dots
\end{array}
$$

где, без ограничения общности, g_1 выбрана как константная функция $g_1 \equiv 0$ и $\overline{z_{i_k}} = \big(g_2(x_{i_k}), \dots, g_n(x_{i_k})\big)$. Таким образом, одна из координатных функций функции G является константной, а остальные $n-1$ функций являются сбалансированными. Заметим, что векторы $y_{i_1}, y_{i_3}, \dots, y_{i_{2^n-1}}$ попарно различны и $y_{i_1} = y_{i_2}, \dots, y_{i_{2^n-1}} = y_{i_{2^n}}$. Следовательно, по построению, все векторы $\{w_1, \dots, w_{2^n}\}$ также попарно различны, следовательно, H является взаимно однозначной.

Обобщим данную конструкцию на случай, когда l координатных булевых функций функции F являются сбалансированными, и любая их линейная комбинация также сбалансирована. Рассмотрим 2-в-1 функцию $F = (f_1, \dots, f_n)$, где $f_{j_1}, \dots, f_{j_l}$ — сбалансированные булевы функции и для любого ненулевого вектора $v \in \mathbb{F}_2^l$ линейная комбинация $v \cdot (f_{j_1}, \dots, f_{j_l})$ является сбалансированной булевой функцией. Согласно Утверждению 1 векторная функция является взаимно однозначной тогда и только тогда, когда любая ее компонентная функция является сбалансированной.

Без ограничения общности рассмотрим случай, когда функции $f_1, \dots, f_l$ сбалансированы, и любая их линейная комбинация также сбалансирована. Тогда мы можем выбрать в качестве первых l координатных функций G константные булевы функции, $g_j \equiv 0$ или $g_j \equiv 1$, где $j = 1, \dots, l$:

$$
\begin{array}{ccccc}
F & & G & & H \\
\dots & & \dots & & \dots \\
y_{i_1} & + & 0,\dots,0,\overline{G(x_{i_1})} & = & w_{i_1} \\
\dots & & \dots & & \dots \\
y_{i_3} & + & 0,\dots,0,\overline{G(x_{i_3})} & = & w_{i_3} \\
\dots & & \dots & & \dots \\
y_{i_2} & + & 0,\dots,0,\overline{G(x_{i_2})} & = & w_{i_2} \\
\dots & & \dots & & \dots \\
y_{i_4} & + & 0,\dots,0,\overline{G(x_{i_4})} & = & w_{i_4} \\
\dots & & \dots & & \dots
\end{array}
$$

где $g_1 \equiv 0, \dots, g_l \equiv 0$ и $\overline{G(x_{i_k})} = \big(g_{l+1}(x_{i_k}), \dots, g_n(x_{i_k})\big)$. Заметим, что для любого выбора функций $g_1, \dots, g_l$ функции $h_1 = f_1 + g_1, \dots, h_l = f_l + g_l$ являются сбалансированными, и, более того, любая ненулевая линейная комбинация $h_1, \dots, h_l$ также является сбалансированной. Первые l координат значения w_k, где $k = 1, \dots, 2^n$ равняются первым l координатам значения y_k, однако, оставшиеся $n - l$ координат зависят от выбора функций $g_{l+1}, \dots, g_n$. Поскольку любая ненулевая линейная комбинация $h_1, \dots, h_l$ сбалансирована, то функции $h_1, \dots, h_l$ являются координатными функциями взаимно однозначной функции. Таким образом, используя вновь приведенный выше метод, мы можем выбрать функции $g_{l+1}, \dots, g_n$ так, что множество векторов $\{w_1, \dots, w_{2^n}\}$ в точности равняется $\mathbb{F}_2^n$, и, следовательно, H — взаимно однозначная функция. Поскольку $F + G = H$, где G — аффинная функция, а H — взаимно однозначная функция, утверждение теоремы доказано.

□

Замечание. *Заметим, что любая аффинная векторная функция из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$ содержит только сбалансированные или константные координатные функции. Следовательно, если функции F и G из Теоремы 1 такие, что F — APN-функция, а G — аффинная функция, тогда $F + G = H$ является APN-перестановкой, поскольку F и H являются EA-эквивалентными функциями. Данное наблюдение демонстрирует важность изучения свойств и методов построения 2-в-1 APN-функций, поскольку это может позволить находить новые APN перестановки.*

2.2 Метод построения допустимых символьных последовательностей

В данном разделе вводится понятие допустимой символьной последовательности, которая представляет вектор значений некоторой 2-в-1 APN-функции. Предложен метод, позволяющий строить всевозможные допустимые последовательности.

2.2.1 Определение и свойства допустимых последовательностей

Пусть F — произвольная векторная 2-в-1 функция из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$. Набор всех ее значений можно разбить на пары совпадающих значений.

Определение 1. Рассмотрим для некоторого натурального числа n набор из 2^{n-1} попарно различных символов $\alpha_1, \ldots, \alpha_{2^{n-1}}$. Будем называть символьную последовательность, состоящую из 2^n символов, *2-в-1 последовательностью*, если она содержит все символы $\alpha_1, \ldots, \alpha_{2^{n-1}}$, и каждый символ встречается в последовательности ровно два раза.

Рассмотрим 2-в-1 последовательность для некоторых символов $\alpha_1, \ldots, \alpha_{2^{n-1}}$ и заметим, что мы можем упорядочить элементы данной последовательности по первому вхождению каждого символа.

Определение 2. Символьная 2-в-1 последовательность для символов $\alpha_1, \ldots, \alpha_{2^{n-1}}$, где $n \in \mathbb{N}$, называется *лексикографически упорядоченной*, если для каждой пары индексов i и j таких, что $i < j$, первое вхождение символа α_i в последовательность предшествует первому вхождению символа α_j.

Нетрудно заметить, что вектору значений произвольной 2-в-1 функции мы можем сопоставить соответствующую 2-в-1 символьную последовательность. Более того, если мы лексикографически упорядочим все 2-в-1 последовательности, то для каждой 2-в-1 векторной функции будет существовать лишь одна соответствующая 2-в-1 последовательность, состоящая из символов $\alpha_1, \ldots, \alpha_{2^{n-1}}$.

Пример 1. Рассмотрим 2-в-1 векторную функцию $F = (1\ 1\ 0\ 0\ 3\ 2\ 3\ 2)$ от трех переменных. Мы можем сопоставить ее вектору значений, например, символьную последовательность $(\alpha_1\ \alpha_1\ \alpha_2\ \alpha_2\ \alpha_3\ \alpha_4\ \alpha_3\ \alpha_4)$, так же, как и символьную последовательность $(\alpha_2\ \alpha_2\ \alpha_3\ \alpha_3\ \alpha_1\ \alpha_4\ \alpha_1\ \alpha_4)$. Первая из приведенных последовательностей является лексикографически упорядоченной, в то время как вторая последовательность таковой не является.

Рассмотрим произвольную APN-функцию F от n переменных. Из определения APN-функции следует, что ее производные $F(x+a)+F(x)$ являются 2-в-1 функциями для любого вектора $a \neq \mathbf{0}$. Тогда, набор значений $\{F(x^{(1)}), \ldots, F(x^{(2^n)})\}$ функции F разбивается данным вектором a на пары $\{F(x^{(i)}), F(x^{(i)}+a)\}$ и все суммы $F(x^{(i)})+F(x^{(i)}+a)$ и $F(x^{(j)})+F(x^{(j)}+a)$ попарно различны для всех $x^{(i)} \neq x^{(j)}$ и $x^{(j)} \neq x^{(i)}+a$. Мы можем перенести данное наблюдение на класс 2-в-1 последовательностей.

Рассмотрим специальные символьные последовательности, соответствующие вектору значений 2-в-1 APN-функции. Заметим, что мы можем рассматривать целое число, обозначающее позицию в последовательности (где самая левая позиция принимается за нулевую), как соответствующий его двоичной записи вектор.

Определение 3. Назовем 2-в-1 последовательность S длины 2^n, где $n \in \mathbb{N}$, *допустимой по направлению*, где a — ненулевой вектор из $\mathbb{F}_2^n$, если пара символов, стоящих на позициях i и $i+a$, отлична от пары символов j и $j+a$ для любых i, j таких, что $i \neq j$ и $i \neq j+a$, и среди всех пар на позициях k и $k+a$ для любого k встретится не более одной пары одинаковых символов (напомним, что здесь рассматривается сложение по модулю 2).

Здесь и далее, если не сказано иначе, мы считаем пары символов неупорядоченными. Рассмотрим 2-в-1 последовательность $(\alpha\ \alpha\ \beta\ \beta\ \gamma\ \delta\ \delta\ \gamma)$. Данная последовательность не является допустимой по направлению $a = (001)$, поскольку в последовательности встречаются пары $\{\alpha, \alpha\}$ и $\{\beta, \beta\}$ на позициях 0 и 1, где $0 = (000)$, $1 = (001) = (000) + (001)$, и на позициях 2 и 3 соответственно, где $2 = (010)$, $3 = (011) = (010) + (001)$. Более того, в последовательности встречается пара $\{\gamma, \delta\}$ на позициях 4 и 5, и пара $\{\delta, \gamma\}$ на позициях 6 и 7, и легко заметить, что эти две пары совпадают. Рассмотрим теперь 2-в-1 последовательность $(\alpha\ \alpha\ \beta\ \gamma\ \beta\ \delta\ \gamma\ \delta)$. Эта последовательность является допустимой по направлению $a = (001)$.

Определение 4. Символьная 2-в-1 последовательность S длины 2^n, где $n \in \mathbb{N}$, называется *допустимой*, если для любого ненулевого вектора $a \in \mathbb{F}_2^n$ она является допустимой по направлению a.

Заметим, что 2-в-1 последовательности, соответствующие вектору значений 2-в-1 APN-функции, всегда являются допустимыми, поскольку, в противном случае, мы имеем противоречие с определением APN-функции.

Определение 5. Символьная 2-в-1 последовательность S_k длины $k \leqslant 2^n$, состоящая из символов $\alpha_1, \ldots, \alpha_{2^{n-1}}$, где $n \in \mathbb{N}$, называется частично допустимой, если

для любого ненулевого $a \in \mathbb{F}_2^n$ она является допустимой по направлению a для всех позиций t таких, что $t \leqslant k$ и $t + a \leqslant k$.

Для некоторой 2-в-1 последовательности S длины 2^n, где $n \in \mathbb{N}$, рассмотрим ее подпоследовательность S_k длины $k \leqslant 2^n$, состоящую из первых k символов последовательности S. Отметим следующий важный факт: для любого $k \leqslant 2^n$ подпоследовательность S_k допустимой последовательности S является частично допустимой. Однако, обратное утверждение является неверным. В качестве примера рассмотрим $n = 3$ и последовательность $S_3 = (\alpha\ \alpha\ \beta)$. Эта последовательность является частично допустимой, однако 2-в-1 последовательность $(\alpha\ \alpha\ \beta\ \beta\ \gamma\ \delta\ \delta\ \gamma)$, содержащая S_3 в качестве подпоследовательности, не является допустимой, как уже было показано выше в Примере 1.

2.2.2 Метод построения всевозможных допустимых последовательностей

В этом подразделе мы приводим описание метода, позволяющего строить всевозможные лексикографически упорядоченные 2-в-1 последовательности фиксированной длины 2^n, где $n \in \mathbb{N}$, состоящие из символов $\alpha_1, \ldots, \alpha_{2^{n-1}}$. Обозначим через C_k множество всех частично допустимых последовательностей длины $k \leqslant 2^n$.

В начале k равняется единице, а множество C_1 состоит только из последовательности (α_1). На каждом шаге по k от C_k к C_{k+1}, пока выполняется условие $k < 2^n$, последовательности $S_k^{(i)}$ из C_k длины k, где $i = 1, \ldots, |C_k|$, дополняются некоторым символом до длины $k + 1$ следующим образом.

Для каждой последовательности $S_k^{(i)}$ в C_k рассмотрим все символы α_j из множества $\{\alpha_1, \ldots, \alpha_{2^{n-1}}\}$ такие, что α_j уже встречался в последовательности $S_k^{(i)}$, но только один раз. Каждый из таких символов добавляется в конец рассмотренной последовательности $S_k^{(i)}$, и проверяется, является ли полученная последовательность длины $k + 1$ частично допустимой.

После этого к последовательности $S_k^{(i)}$ также добавляется символ α_r, который не встречался в последовательности $S_k^{(i)}$ и является лексикографически наименьший среди всех символов из $\{\alpha_1, \ldots, \alpha_{2^{n-1}}\}$, которые еще не встречались в $S_k^{(i)}$. Вновь проверяется, является ли полученная из $S_k^{(i)}$ и символа α_r последовательность длины $k + 1$ частично допустимой.

Все полученные частично допустимые последовательности добавляются в множество C_{k+1}. На последнем шаге мы получаем множество, состоящее из всех частично допустимых последовательностей длины $k = 2^n$, а значит, из всех

допустимых последовательностей. Мы приводим формальное описание данного метода (см. Метод 1).

$k \leftarrow 1$
$C_1 \leftarrow \{(\alpha_1)\}$
до тех пор, пока $k < 2^n$ **выполнять**
  для всех $S_k^{(i)} = (\alpha_{i_1}, \ldots, \alpha_{i_k})$ *из* C_k **выполнять**
    цикл $j = 1$ **до** 2^{n-1} **выполнять**
      если $j = i_t$ *для некоторого* $t \in \{1, \ldots, k\}$ ***и*** α_j *встречается* $S_k^{(i)}$ *один раз* ***ИЛИ*** $j \neq i_1, \ldots, j \neq i_k$ ***и*** α_j *— лексикографически наименьший символ* **тогда**
        $S_{k+1}^* = (\alpha_{i_1}, \ldots, \alpha_{i_k}, \alpha_j)$
        если S_{k+1}^* *— частично допустимая* **тогда**
          $C_{k+1} \leftarrow C_{k+1} \cup \{S_{k+1}^*\}$
        конец
      конец
    конец
  $k \leftarrow k + 1$
конец

Метод 1: Метод построения всевозможных допустимых последовательностей

Докажем, что все существующие допустимые последовательности фиксированной длины будут получены с помощью данного метода.

Утверждение 1. *Лексикографически упорядоченная 2-в-1 последовательность* S *длины* 2^n*, где* $n \in \mathbb{N}$*, состоящая из символов* $\alpha_1, \ldots, \alpha_{2^{n-1}}$*, является допустимой тогда и только тогда, когда она получена методом, описанным в Методе 1.*

Доказательство. Заметим, что на каждом шаге от C_k к C_{k+1}, где $k = 1, \ldots, 2^n$, любой добавляемый символ α_j либо уже встречался в рассматриваемой последовательности, либо еще не встречался и является лексикографически наименьшим символом среди символов не из последовательности, таким образом, в результате будут получены лишь лексикографически упорядоченные 2-в-1 последовательности.

$\Leftarrow$ На последнем шаге от C_{2^n-1} к C_{2^n} мы добавляем в C_{2^n} частично допустимые последовательности длины 2^n. Поскольку любая частично допустимая последовательность длины 2^n является допустимой по определению, все последовательности, лежащие в C_{2^n} в конце реализации данного метода, будут являться допустимыми.

$\Rightarrow$ Рассмотрим произвольную лексикографически упорядоченную последовательность S, состоящую из символов $\alpha_1, \ldots, \alpha_{2^{n-1}}$, где первый символ последовательности — это α_1. Любая подпоследовательность длины $k < 2^n$, состоящая

из первых k символов последовательности S, является частично допустимой и также начинается с символа α_1. Легко заметить, что для любой частично допустимой последовательности S_{k+1} из множества C_{k+1}, подпоследовательность S_k, состоящая из первых k символов последовательности S_{k+1}, лежит в множестве C_k, поскольку она является частично допустимой последовательностью длины k. Таким образом, на каждом шаге мы строим всевозможные частично допустимые последовательности, которые начинаются с символа α_1, и рассматриваемая последовательность S будет лежать в C_{2^n}.

□

В Таблице 2.1 мы приводим некоторые примеры допустимых последовательностей, полученных с помощью описанного выше метода.

Таблица 2.1: Примеры построенных допустимых последовательностей.

$n=3:$	α_1	α_2	α_3	α_3	α_4	α_2	α_4	α_1								
$n=4:$	α_1	α_1	α_2	α_3	α_2	α_4	α_3	α_5	α_4	α_5	α_6	α_7	α_7	α_8	α_6	α_8
$n=5:$	α_1	α_2	α_1	α_3	α_2	α_4	α_5	α_6	α_7	α_8	α_9	α_{10}	α_9	α_{11}	α_{12}	α_4
	α_3	α_8	α_{13}	α_{14}	α_{15}	α_{15}	α_{11}	α_{16}	α_6	α_{12}	α_5	α_{10}	α_7	α_{14}	α_{16}	α_{13}
$n=6:$	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8	α_3	α_5	α_9	α_9	α_{10}	α_6	α_{11}	α_1
	α_{10}	α_2	α_4	α_7	α_{12}	α_8	α_{12}	α_{13}	α_{14}	α_{13}	α_{11}	α_{14}	α_{15}	α_{16}	α_{17}	α_{18}
	α_{19}	α_{20}	α_{21}	α_{22}	α_{23}	α_{24}	α_{18}	α_{19}	α_{25}	α_{24}	α_{20}	α_{26}	α_{27}	α_{28}	α_{29}	α_{30}
	α_{29}	α_{31}	α_{30}	α_{28}	α_{31}	α_{32}	α_{32}	α_{25}	α_{26}	α_{22}	α_{27}	α_{21}	α_{23}	α_{16}	α_{15}	α_{17}

2.3 Построение 2-в-1 APN-функций

В данном разделе мы рассматриваем способ построения 2-в-1 APN-функций из допустимых последовательностей. Описан метод поиска APN-перестановок, использующий 2-в-1 APN-функции.

2.3.1 Означенные последовательности

Для того, чтобы получить из допустимой последовательности 2-в-1 функцию, в общем случае каждому символу последовательности мы должны сопоставить некоторое значение из $\mathbb{F}_2^n$. Наша цель — построить именно 2-в-1 APN-функции, поэтому необходимо подобрать это означивание таким образом, что свойство функции быть APN-функцией не будет нарушаться. Рассмотрим множество символов $\{\alpha_1, \ldots, \alpha_{2^{n-1}}\}$, где $n \in \mathbb{N}$, и произвольное подмножество $C \subset \mathbb{F}_2^n$ такое, что $|C| = 2^{n-1}$ и $C = \{x^{(1)}, \ldots, x^{(2^{n-1})}\}$.

Определение 6. Взаимно однозначная функция O из множества $\{\alpha_1, \ldots, \alpha_{2^{n-1}}\}$ на подмножество $C = \{x^{(1)}, \ldots, x^{(2^{n-1})}\}$, где $n \in \mathbb{N}$, называется *означиванием*.

Рассмотрим допустимую последовательность S длины 2^n, состоящую из символов $\alpha_1, \ldots, \alpha_{2^{n-1}}$.

Определение 7. Допустимая последовательность S длины 2^n, где $n \in \mathbb{N}$, называется *означенной*, если к каждому символу α_i, где $i = 1, \ldots, 2^{n-1}$, последовательности S применено некоторое означивание $O(\alpha_i)$.

Далее будем говорить, что означенная последовательность S длины 2^n, где $n \in \mathbb{N}$, означена векторами $x^{(1)}, \ldots, x^{(2^{n-1})}$, если $O(\alpha_1) = x^{(1)}, \ldots, O(\alpha_{2^{n-1}}) = x^{(2^{n-1})}$.

Рассмотрим произвольную последовательность S длины 2^n, где $n \in \mathbb{N}$. Поскольку для каждого выбранного подмножества C существует $2^{n-1}!$ различных означенных последовательностей, в дальнейшем мы будем рассматривать упорядоченные наборы векторов из $\mathbb{F}_2^n$, каждому из которых можно поставить во взаимно однозначное соответствие некоторую означенную последовательность. Заметим, что означенная последовательность представляет собой вектор значений некторой 2-в-1 векторной функции. Следующее утверждение показывает, как можно выбрать набор значений при $n = 3$ для того, чтобы получить из последовательности 2-в-1 APN-функцию.

Утверждение 2. *Последовательность, означенная векторами c_1, c_2, c_3, c_4 из $\mathbb{F}_2^3$, является вектором значений 2-в-1 APN-функции тогда и только тогда, когда для данных векторов выполнено соотношение $c_1 + c_2 + c_3 + c_4 \neq \boldsymbol{0}$.*

Доказательство. Рассмотрим произвольную допустимую последовательность S, состоящую из символов $\{\alpha, \beta, \gamma, \delta\}$, которая означена векторами c_1, c_2, c_3, c_4 из $\mathbb{F}_2^n$.

$\Leftarrow$ Пусть для данных векторов выполнено соотношение $c_1 + c_2 + c_3 + c_4 \neq \mathbf{0}$. Для некоторого ненулевого вектора a рассмотрим сумму символов на позициях i и $i + a$ и сумму символов на позициях j и $j + a$ для некоторых i, j таких, что $i \neq j$ и $i \neq j + a$. Поскольку последовательность S — допустимая, без ограничения общности, для таких сумм возможны следующие случаи:

$\{\alpha + \alpha, \beta + \gamma\}$;

$\{\alpha + \beta, \alpha + \gamma\}$;

$\{\alpha + \beta, \gamma + \delta\}$.

Теперь заменим символы последовательности S соответствующими векторами c_1, c_2, c_3, c_4. Напомним, что векторная функция F является APN-функцией

тогда и только тогда, когда для любого ненулевого вектора a и для любых таких аргументов x и x', что $x \neq x'$ и $x \neq x'+a$, суммы $F(x)+F(x+a)$ и $F(x')+F(x'+a)$ различны. Нетрудно заметить, что в первом и втором случае функция, имеющая такой вектор значений, будет являться APN-функцией, поскольку все векторы c_i, $i = 1, 2, 3, 4$ попарно различны, и, следовательно, различны полученные суммы. А условие $c_1 + c_2 + c_3 + c_4 \neq \mathbf{0}$ гарантирует, что суммы и в третьем случае не будут равны. Таким образом, означенная последовательность является вектором значений 2-в-1 APN-функции.

$\Rightarrow$ Пусть означенная последовательность является вектором значений 2-в-1 APN-функции. Рассмотрим производную этой функции по некоторому ненулевому направлению a. Напомним, что поскольку F — APN-функция, то ее производная $D_aF(x) = F(x+a) + F(x)$ является 2-в-1 функцией, а, значит, вектор значений функции F разбивается на такие пары значений $\{(F(x), F(x+a)) \mid x \in \mathbb{F}_2^n\}$, что сумма значений из каждой пары единственна. Тогда при $n = 3$ для такого разбиения на пары без ограничения общности возможны два случая.

В первом случае среди таких пар присутствует одна пара совпадающих значений, скажем, пара (c_1, c_1), и, таким образом, их сумма равна нулю. Заметим, что это единственная возможная пара совпадающих значений, поскольку иначе две различные пары в сумме дадут одинаковое значение, что противоречит свойству функции быть APN-функцией. Так как всего имеется четыре пары, из которых одна пара содержит два совпадающих значения, то остальные три пары содержат три значения c_2, c_3, c_4, и, следовательно, для любых двух пар найдется значение c_i такое, что оно встречается в обеих парах:

(c_1, c_1);
(c_2, c_3);
(c_2, c_4);
(c_3, c_4).

Во втором случае значения в каждой паре различны, поэтому всегда найдутся две пары, в которых встретятся все четыре значения. В примере ниже это пары (c_1, c_3) и (c_2, c_4):

(c_1, c_2);
(c_1, c_3);
(c_2, c_4);
(c_2, c_3).

Заметим, что первый случай может реализоваться не более четырех раз, поскольку пара (c_i, c_i), для каждого $i = 1, 2, 3, 4$, не может встретиться среди значений более, чем одной производной. Следовательно, для некоторого ненулевого

вектора a гарантированно реализуется второй случай. Рассмотрим соответствующие пары и выберем из них две пары значений, которые содержат все четыре вектора c_1, c_2, c_3, c_4. Без ограничения общности, рассмотрим пары (c_1, c_3) и (c_2, c_4). Поскольку F — APN-функция, то сумма значений каждой пары различна и, следовательно, $c_1 + c_2 \neq c_3 + c_4$, что доказывает утверждение.

□

Замечание 1. *Рассмотрим произвольное упорядоченное множество C двоичных векторов длины n такое, что $|C| = 2^{n-1}$ и сумма любых четырех векторов из C не равна нулю. Из Теоремы 2 следует, что допустимая последовательность, означенная векторами из C, является APN-функцией. Однако, из Теоремы 9 следует, что $|C| \leqslant \sqrt{2^{n+1} - 1} + 1$, следовательно, $|C| < 2^{n-1}$, когда $n \geqslant 4$. Таким образом, при больших размерностях для означивания необходимо непосредственно проверять все возможные упорядоченные множества C из $\mathbb{F}_2^n$, такие, что $|C| = 2^{n-1}$.*

2.3.2 Общий случай поиска небходимого означивания

Как было рассмотрено выше, в общем случае нам требуется выбрать упорядоченный набор векторов из $\mathbb{F}_2^n$ и заменить символы в рассматриваемой допустимой последовательности соответствующими векторами. Таким образом, полный перебор всех возможных наборов векторов может быть разделен на два последовательных шага. На первом шаге необходимо выбрать некоторое множество C, содержащее 2^{n-1} векторов из $\mathbb{F}_2^n$, тогда мы имеем $C_{2^n}^{2^{n-1}}$ способов осуществить такой выбор. Второй шаг заключается в том, что мы для всех возможных перестановок каждого из множеств C проверяем, является ли полученная означенная последовательность APN-функцией. Следующая гипотеза потенциально позволяет сократить полный перебор за счет второго шага. Рассмотрим множество C^*, состоящее из $C_{2^n}^{2^{n-1}}$ всевозможных упорядоченных наборов $C \subset \mathbb{F}_2^n$ мощности $|C| = 2^{n-1}$ таких, что все векторы в C лексикографически упорядочены.

Гипотеза 1. *Пусть S — допустимая последовательность длины 2^n. Если 2-в-1 векторная функция с вектором значений, полученным в результате означивания последовательности S, не является APN-функцией для всех упорядоченных наборов C из C^*, то в $\mathbb{F}_2^n$ не существует упорядоченного набора из 2^{n-1} элементов, такого, что последовательность S, означенная при помощи векторов из этого набора, является 2-в-1 APN-функцией.*

Данное предположение вычислительно доказано для $n = 4$ и для некоторых примеров размерности $n = 5, 6$. Также вычислительно получен следующий результат:

Утверждение 3. *Не существует 2-в-1 APN-функций от 4 переменных.*

Замечание. *Напомним, что также не существует взаимно однозначных APN-функций от 4 переменных.*

2.3.3 Поиск APN-перестановок, которые EA-эквивалентны 2-в-1 APN-функциям

Как было показано в Разделе 2.1, для 2-в-1 APN-функции F всегда найдутся векторные функции, каждая координатная булева функция которых сбалансирована или константна, что их сумма с функцией F дает взаимно однозначную функцию. Таким образом, если одна из таких функций окажется аффинной, то в результате мы получим APN-перестановку. Следовательно, для фиксированной 2-в-1 APN-функции F нужно проверить, существует ли аффинная векторная функция A такая, что их сумма $H = F + A$ является APN-перестановкой. Заметим, что достаточно перебирать только линейные векторные функции, поскольку прибавление константы не влияет на взаимную однозначность функции H. Данные наблюдения позволяют предложить новый метод поиска APN-перестановок от n переменных. Далее мы приводим описание данного метода (Метод 2). Через P_n будем обозначать множество APN-перестановок от n переменных, полученное в результате реализации данного метода.

2.3.4 Примеры

Для $n = 5$ мы нашли 2-в-1 функции, EA-эквивалентные всем известным (с точностью до аффинной эквивалентности, см. [21]) APN-перестановкам. В Таблице 2.2 мы приводим построенные 2-в-1 APN-функции и соответствующие им линейные векторные функции такие, что суммы $F_i + L_i$ являются взаимно однозначными APN-функциями.

Также мы нашли пример (см. Таблицу 2.3) 2-в-1 APN-функции F, которая EA-эквивалентна единственной известной APN-перестановке от 6 переменных, а также соответствующую линейную векторную функцию L.

$P_n \leftarrow \varnothing$
для всех *допустимых последовательностей* $S^{(t)}$ *длины* 2^n **выполнять**
  для всех *подмножеств* $C \subset \mathbb{F}_2^n$ *таких, что* $|C| = 2^{n-1}$, **выполнять**
    для всех *перестановок* $\pi^{(j)}$ *множества* $C = \{x_{i_1}, \ldots, x_{i_{2^n-1}}\}$ **выполнять**
      означиваем допустимую последовательность $S^{(t)}$ упорядоченным набором векторов $\{\pi^{(j)}(x_{i_1}), \ldots, \pi^{(j)}(x_{i_{2^n-1}})\}$
      $F \leftarrow S^{(t)}$, где $S^{(t)}$ — уже означенная последовательность.
      если F — *APN-функция* **тогда**
        для всех *линейных векторных функций* L *от* n *переменных* **выполнять**
          $H \leftarrow F + L$
          если H — *взаимно однозначная* **тогда**
            $P_n \leftarrow P_n \cup H$
          конец
        конец
      конец
    конец
  конец
конец

Метод 2: Метод поиска взаимно однозначных APN-функций

Таблица 2.2: Все (с точностью до аффинной эквивалентности) 2-в-1 APN функции от 5 переменных, EA-эквивалентные перестановкам, и соответствующие линейные функции такие, что $F_i + L_i$ — APN-перестановки.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
F_1	0	14	22	31	4	14	27	12	6	6	24	3	23	22	15	11
	5	31	15	12	9	4	9	2	27	5	2	23	24	0	3	11
L_1	0	15	20	27	7	8	19	28	3	12	23	24	4	11	16	31
	2	13	22	25	5	10	17	30	1	14	21	26	6	9	18	29
F_2	0	5	29	31	24	23	9	16	5	15	10	4	12	16	23	30
	26	4	30	14	31	24	22	14	22	9	15	29	0	26	12	10
L_2	0	4	31	27	27	31	4	0	0	4	31	27	27	31	4	0
	28	24	3	7	7	3	24	28	28	24	3	7	7	3	24	28
F_3	0	27	25	5	11	26	30	25	2	12	0	29	17	27	12	4
	11	4	29	24	26	2	18	17	24	10	30	18	5	14	14	10
L_3	0	26	27	1	8	18	19	9	7	29	28	6	15	21	20	14
	13	23	22	12	5	31	30	4	10	16	17	11	2	24	25	3
F_4	0	16	27	12	12	22	6	27	6	24	3	26	30	10	10	25
	0	3	18	22	26	19	25	23	30	19	18	24	16	23	13	13
L_4	0	17	25	8	15	30	22	7	3	18	26	11	12	29	21	4
	6	23	31	14	9	24	16	1	5	20	28	13	10	27	19	2
F_5	0	29	26	0	6	17	13	29	3	16	4	16	18	11	4	26
	1	14	7	15	20	17	3	1	15	14	20	18	13	6	7	11
L_5	0	28	24	4	5	25	29	1	6	26	30	2	3	31	27	7
	7	27	31	3	2	30	26	6	1	29	25	5	4	24	28	0

Таблица 2.3: Пример 2-в-1 APN-функции F, которая EA-эквивалентна известной APN-перестановке от 6 переменных, а также соответствующая линейная функция L.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	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	58	59	60	61	62	63
F	54	52	48	57	14	39	34	0	63	45	45	0	2	33	32	28
	55	1	6	46	5	46	28	8	37	57	5	19	2	25	48	32
	17	54	58	58	33	1	34	14	51	21	8	29	55	12	30	29
	27	19	21	37	17	40	63	52	40	27	51	12	6	30	39	25
L	0	52	0	52	1	53	1	53	0	52	0	52	1	53	1	53
	63	11	63	11	62	10	62	10	63	11	63	11	62	10	62	10
	63	11	63	11	62	10	62	10	63	11	63	11	62	10	62	10
	0	52	0	52	1	53	1	53	0	52	0	52	1	53	1	53

Глава 3

Дифференциально 4-равномерные 2-в-1 функции как подфункции APN перестановок

Поскольку о взаимно однозначных APN-функциях при четных размерностях известно не так много, одно из перспективных направлений заключается в изучении свойств их компонентных и координатных функций. В данной главе рассматриваются 2-в-1 векторные функции, которые изоморфны $(n-1)$-подфункциям APN-перестановок. Доказывается, что любая такая 2-в-1 функция является дифференциально 4-равномерной и что любая $(n-1)$-подфункция APN-перестановки структурно является допустимой последовательностью и может быть получена при помощи Метода 1, который предложен в предыдущей главе. Также описывается новый метод (см. Метод 3), осуществляющий поиск взаимно однозначных APN-функций с помощью 2-в-1 функций, изоморфных их подфункциям.

На первом шаге данного метода строятся всевозможные допустимые последовательности. Далее эти последовательности означиваются из множества $\{0,\dots,2^{n-1}-1\}$ и рассматриваются как векторы значений векторных 2-в-1 функций, из которых далее выбираются дифференциально 4-равномерные функции, которым, как доказывается, можно сопоставить $(n-1)$-подфункции взаимно однозначных функций. Для того, чтобы получить APN-перестановку, необходимо перебрать булевы функции f специального вида и проверить, является ли APN-функцией взаимно однозначная функция, построенная из рассматриваемой $(n-1)$-подфункции и координатной функции f.

Ввиду того, что при $n \geqslant 7$ поиск таких координатных функций слишком трудоемкий, необходимо оценить число тех координатных функций, для которых полученная взаимно однозначная функция является APN-функцией. С целью получения оценки для взаимно однозначной функции вводится понятие ассоци-

ированной перестановки. Доказывается теорема о том, что взаимно однозначная функция является APN-функцией тогда и только тогда, когда ее ассоциированная перестановка также является APN-функцией. Получена необходимая оценка на число требуемых координатных функций.

3.1 Предварительные сведения

Рассмотрим произвольную векторную функцию $F = (f_1, \ldots, f_n)$ из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$.

Определение 8. Векторная функция $F_j^{'}$ из $\mathbb{F}_2^n$ в $\mathbb{F}_2^{n-1}$ называется $(n-1)$-*подфункцией* функции F, если $F_j^{'} = (f_1, \ldots, f_{j-1}, f_{j+1}, \ldots, f_n)$ для некоторого $j \in \{1, \ldots, n\}$.

Напомним, что векторному пространству $\mathbb{F}_2^n$ можно поставить во взаимно однозначное соответствие целочисленное множество $\{0, \ldots, 2^n - 1\}$, где каждое число есть соответствующее представление двоичного вектора из $\mathbb{F}_2^n$. Мы можем рассматривать произвольную $(n-1)$-подфункцию $F_j^{'}$ из $\mathbb{F}_2^n$ в $\mathbb{F}_2^{n-1}$ как векторную функцию из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$, которая принимает значения исключительно из множества $\{0, \ldots, 2^{n-1} - 1\}$ и, таким образом, изоморфна функции $F_j^{'}$. Далее, под "$(n-1)$-подфункцией" функции F от n переменных мы имеем в виду функцию из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$, которая изоморфна соответствующей подфункции функции F. Рассмотрим 2-в-1 функцию, которая принимает значения из множества $\{0, \ldots, 2^{n-1} - 1\}$. Нетрудно заметить, что вектор значений такой функции может быть представлен в виде некоторой перестановки целочисленного набора $(0, 0, 1, 1, \ldots, 2^{n-1} - 1, 2^{n-1} - 1)$. Будем обозначать множество таких 2-в-1 векторных функции от n переменных с помощью $\mathcal{T}_n$.

Замечание. *Заметим, что любая* $(n-1)$*-подфункция взаимно однозначной векторной функции — функция из множества* $\mathcal{T}_n$.

3.2 Подфункции взаимно однозначных APN-функций

3.2.1 Дифференциальная равномерность 2-в-1 функций специального вида

Характеризация APN-функций через подфункции была исследована А. Городиловой в работе [3]. Автором было получено, что любая подфункция APN-функции от n переменных, действующая из $\mathbb{F}_2^{n-1}$ в $\mathbb{F}_2^{n-1}$, является APN-функцией или дифференциально 4-равномерной. Следующее утверждение пе-

реносит данный результат на случай, когда рассматриваются подфункции APN-перестановок, действующие из $\mathbb{F}_2^n$ в $\mathbb{F}_2^{n-1}$.

Утверждение 4. *Пусть F — взаимно однозначная APN-функция от n переменных. Тогда любая из ее $(n-1)$-подфункций является 2-в-1 APN-функцией или 2-в-1 дифференциально 4-равномерной функцией.*

Доказательство. Рассмотрим функцию $F(x) = \big(f_1(x), \dots, f_n(x)\big)$. Поскольку F является APN-функцией, ее производная $D_aF(x) = F(x+a)+F(x) = \big(f_1(x+a)+ f_1(x), \dots, f_n(x+a) + f_n(x)\big)$ — 2-в-1 векторная функция для каждого ненулевого вектора a. Без ограничения общности рассмотрим одну из таких производных и множество ее значений $\{y^{(1)}, \dots, y^{(2^{n-1})}\}$, где каждое значение принимается два раза:

$$\begin{array}{cccc}
y_1^{(1)} & y_2^{(1)} & \dots & y_n^{(1)} \\
\dots & \dots & \dots & \dots \\
y_1^{(1)} & y_2^{(1)} & \dots & y_n^{(1)} \\
\dots & \dots & \dots & \dots \\
y_1^{(2^{n-1})} & y_2^{(2^{n-1})} & \dots & y_n^{(2^{n-1})} \\
\dots & \dots & \dots & \dots \\
y_1^{(2^{n-1})} & y_2^{(2^{n-1})} & \dots & y_n^{(2^{n-1})}
\end{array}$$

Рассмотрим произвольную $(n-1)$-подфункцию F_j' и ее производную по тому же направлению. Нетрудно заметить, что, поскольку только одна координатная функция удалена, каждое из значений данной производной не может встретиться более четырех раз, кроме того, случай, когда производная принимает некоторое значение ровно 4 раза, возможен, только если векторы $y_1^{(k_1)}, y_2^{(k_1)}, \dots, y_n^{(k_1)}$ и $y_1^{(k_2)}, y_2^{(k_2)}, \dots, y_n^{(k_2)}$ для некоторого $k_1 \neq k_2$ отличаются только по j-ой координате. Это доказывает утверждение. □

Лемма 1. *Пусть F — произвольная 2-в-1 векторная функция из $\mathcal{T}_n$, где $n \in \mathbb{N}$. Тогда максимальное число ненулевых векторов a, таких, что D_aF является 2-в-1 функцией, равно 2^{n-1}.*

Доказательство. Пусть производная $D_aF(x) = F(x+a) + F(x)$ по некоторому ненулевому направлению a является 2-в-1 функцией. Заметим, что, поскольку, F — функция из множества $\mathcal{T}_n$, производная D_aF также является функцией из $\mathcal{T}_n$, таким образом, среди значений функции D_aF обязательно встретится $\mathbf{0}$, и, следовательно,$F(x^{(1)} + a) = F(x^{(1)})$ для некоторых $x^{(1)}$ и $x^{(2)} = x^{(1)} + a$ из $\mathbb{F}_2^n$. Поскольку D_aF — 2-в-1 функция, не существует такого $x^{(3)}$ в $\mathbb{F}_2^n$, где $x^{(3)} \neq x^{(1)}$

и $x^{(3)} \neq x^{(2)}$, что $F(x^{(3)} + a) = F(x^{(3)})$. Легко заметить, что если $a' \neq a''$, и выполнено $F(x' + a') = F(x')$ и $F(x'' + a'') = F(x'')$ для некоторых x', x'' из $\mathbb{F}_2^n$, тогда $x' \neq x''$, $x' \neq x'' + a''$, $x' + a' \neq x''$ и $x' + a' \neq x'' + a''$, так как F — 2-в-1 функция. Поскольку существует только 2^{n-1} таких различных пар векторов из $\mathbb{F}_2^n$, то максимальное число таких ненулевых векторов a, что $D_a F$ является 2-в-1 функцией, равно 2^{n-1}.

□

Замечание. *Интересно, что данная оценка достигается на* $(n-1)$*-подфункциях APN-функций Голда для нечетных* $n \leqslant 7$*. В работах [18] и [19] обсуждается понятие локальной APN-функции. Функция* F *над конечным полем называется локальной APN-функцией, если для всех* $b \in GF(2^n)$ *таких, что* $b \neq 0, 1$*, выполнено* $\delta(1, b) \leqslant 2$*. В некотором смысле эти функции находятся на минимальном «расстоянии» от класса APN-функций и, соответственно, могут обеспечивать лучшую защиту от дифференциальной атаки среди всех остальных дифференциально 4-равномерных функций. Поэтому, рассмотрение числа 2-в-1 функций среди производных дифференциально 4-равномерной функции может быть целесообразным также в контексте «расстояния» от класса APN-функций.*

Следующее утверждение является непосредственным следствием из Утверждения 4 и Леммы 1.

Теорема 2. *Пусть* F *— APN-перестановка от* n *переменных. Тогда любая из ее* $(n-1)$*-подфункций является дифференциально 4-равномерной векторной функцией из множества* $\mathcal{T}_n$*.*

3.2.2 $(n-1)$-подфункции APN-перестановок и допустимые символьные последовательности

Были получены следующие наблюдения относительно $(n-1)$-подфункций APN-перестановок. Мы проверили все известные (с точностью до аффинной эквивалентности) APN-перестановки вплоть до $n = 7$, включая APN-функцию Диллона, и для каждой рассмотренной APN-перестановки было обнаружено, что векторы значений 2-в-1 функций, соответствующих любым ее $(n-1)$-подфункциям, могут быть получены из 2-в-1 допустимых последовательностей, и, таким образом, могут быть найдены с помощью метода, описанного в Алгоритме 1. Далее мы доказываем это свойство для $(n-1)$-подфункций APN-перестановок для произвольного n.

Теорема 3. *Пусть F — APN-перестановка от n переменных. Тогда, 2-в-1 символьная последовательность, соответствующая вектору значений любой $(n-1)$-подфункции перестановки F, является допустимой.*

Доказательство. Рассмотрим взаимно однозначную APN-функцию $F = (f_1, \ldots, f_n)$. Без ограничения общности рассмотрим ее подфункцию $F' = (f_1, \ldots, f_{n-1})$. Пусть $S = (\alpha_{i_0}, \ldots, \alpha_{i_{2^n-1}})$ — 2-в-1 символьная последовательность, соответствующая вектору значений подфункции F', где $i_0, \ldots, i_{2^n-1}$ — индексы из множества $\{1, \ldots, 2^{n-1}\}$. Заметим, что здесь $F'(x^{(k)})$ соответствует символу α_{i_k} на позиции с номером $k = 0, \ldots, 2^n - 1$, где $x^{(k)}$ — двоичное представление числа k. Предположим, что последовательность S не является допустимой, следовательно, существует такой ненулевой вектор a, что последовательность S не является допустимой по направлению a, следовательно, возможны два случая.

Рассмотрим первый случай. Предположим, что найдутся два целых числа i и j, где $i \neq j$ и $i + a \neq j$, такие, что два символа, стоящие на позициях i и $i + a$, являются одинаковыми, пусть это, например, символы (α, α). Аналогично, пусть также найдутся два символа на позициях j и $j + a$, пусть это символы (β, β). Следовательно, $F'(x^{(i)}) = F'(x^{(i)} + a) = y^{(i)}$ и $F'(x^{(j)}) = F'(x^{(j)} + a) = y^{(j)}$ для некоторых векторов $y^{(i)}$ и $y^{(j)}$ из $\mathbb{F}_2^{n-1}$, где $y^{(i)} \neq y^{(j)}$. Поскольку F — взаимно однозначная функция, без ограничения общности $F(x^{(i)}) = (y^{(i)}, 1)$ и $F(x^{(i)} + a) = (y^{(i)}, 0)$. Для второй пары мы получаем, что $F(x^{(j)}) = (y^{(j)}, 1)$ и $F(x^{(j)} + a) = (y^{(j)}, 0)$. Следовательно, для производной $D_a F$ выполнено $D_a F(x^{(i)}) = F(x^{(i)}) + F(x^{(i)} + a) = (0, \ldots, 0, 1) = F(x^{(j)}) + F(x^{(j)} + a) = D_a F(x^{(j)})$, таким образом, F не является APN-функцией.

Теперь рассмотрим второй случай. Предположим, что найдутся два целых числа i и j, где $i \neq j$ и $i + a \neq j$, таких, что пара символов, стоящих на позициях i и $i + a$, совпадает с парой символов, стоящих на позициях j и $j + a$, пусть это, например, пара (α, β). Следовательно, поскольку F — взаимно однозначная функция, без ограничения общности для двух различных векторов $y^{(k)}$ и $y^{(l)}$ из $\mathbb{F}_2^{n-1}$ есть две возможности:

$F(x^{(i)}) = (y^{(k)}, 1)$ и $F(x^{(i)} + a) = (y^{(l)}, 1)$;
$F(x^{(j)}) = (y^{(k)}, 0)$ и $F(x^{(j)} + a) = (y^{(l)}, 0)$;
или
$F(x^{(i)}) = (y^{(k)}, 0)$ и $F(x^{(i)} + a) = (y^{(l)}, 1)$;
$F(x^{(j)}) = (y^{(k)}, 1)$ и $F(x^{(j)} + a) = (y^{(l)}, 0)$.

В обоих случаях выполнено $D_a F(x^{(i)}) = D_a F(x^{(j)})$, следовательно, F не является APN-функцией. □

Учитывая результаты Теоремы 2, мы можем обобщить результаты, полученные в Теореме 3, в следующую гипотезу.

Гипотеза 2. *Пусть F — дифференциально 4-равномерная функция из $\mathcal{T}_n$. Тогда, 2-в-1 символьная последовательность, соответствующая вектору значений функции F, является допустимой.*

Данная гипотеза вычислительно доказана для случая $n = 3$. Также, для $n = 4$ получен следующий результат.

Утверждение 5. *Не существует дифференциально 4-равномерных векторных булевых функций в множестве $\mathcal{T}_4$.*

Напомним, что взаимно однозначных APN-функций от 4 переменных также не существует.

3.3 Метод построения взаимно однозначных APN-функций

3.3.1 Описание метода

Заметим, что поскольку справедлива Теорема 3, каждая APN-перестановка может быть получена из 2-в-1 дифференциально 4-равномерной функции, вектор значений которой структурно является допустимой последовательностью. Таким образом, следующий метод для поиска APN-перестановок может быть предложен.

Мы перебираем всевозможные допустимые последовательности и проверяем параметр дифференциальной равномерности для каждой означенной последовательности S (которая означивается при помощи значений $\{0, \ldots, 2^{n-1}-1\}$). Если S — дифференциально 4-равномерная, то она потенциально изоморфна $(n-1)$-подфункции некоторой APN-перестановки. Следовательно, остается подобрать недостающую координатную булеву функцию f, такую, что взаимно однозначная функция, построенная из данной $(n-1)$-подфункции и функции f, является APN-функцией. Поймем, сколько булевых функций необходимо проверить.

Рассмотрим $(n-1)$-подфункцию $F_j' = (f_1, \ldots, f_{j-1}, f_{j+1}, \ldots, f_n)$ произвольной взаимно однозначной векторной функции и сбалансированную булеву функцию f от n переменных. Все значения F_j' можно разбить на 2^{n-1} пар одинаковых значений. Рассмотрим такую пару значений y_i, где $y_i = F_j'(x_{i_1}) = F_j'(x_{i_2})$. Нетрудно заметить, что функция $H = (f_1, \ldots, f_{j-1}, f, f_{j+1}, \ldots, f_n)$ является взаимно однозначной тогда и только тогда, когда для любого i из $\{0, 1, \ldots, 2^{n-1}-1\}$ выполнено

$f(x_{i_m}) = 0$ и $f(x_{i_l}) = 1$ для индексов $m, l \in \{1, 2\}$, таких, что $m \neq l$. Следовательно, для каждой пары одинаковых значений подфункции есть две возможности разместить значения 0 и 1 недостающей координатной функции. Поскольку имеется 2^{n-1} пар одинаковых значений, то существует $2^{2^{n-1}}$ булевых функций f таких, что функция H — взаимно однозначна. Ниже мы приводим формальное описание данного метода (см. Метод 3).

$P_n \leftarrow \varnothing$
для всех *допустимых последовательностей* $S^{(t)}$ *длины* 2^n **выполнять**
  для всех *перестановок* $\pi^{(j)}$ *множества* $C = \{0, 1, \ldots, 2^{n-1}\}$ **выполнять**
    означиваем допустимую последовательность $S^{(t)}$ упорядоченным набором векторов $\{\pi^{(j)}(0), \ldots, \pi^{(j)}(2^{n-1})\}$
    $F^{(j)} \leftarrow S^{(t)}$, где $S^{(t)}$ — уже означенная последовательность.
    если $F^{(j)}$ — *дифференциально 4-равномерная* **тогда**
      для всех $2^{2^{n-1}}$ *возможных координатных булевых функций* f **выполнять**
        $H \leftarrow F^{(j)} \cup f = (f_1, \ldots, f_{j-1}, f, f_{j+1}, \ldots, f_n)$
        если H — *APN-функция* **тогда**
          $P_n \leftarrow P_n \cup \{H\}$
        конец
      конец
    конец
  конец
конец

Метод 3: Метод поиска APN-перестановок с помощью дифференциально 4-равномерных 2-в-1 функций

Замечание 2. *По сравнению с первым методом поиска APN-перестановок, мы выигрываем в трудоемкости за счет отсутствия проверки всевозможных подмножеств $C \in \mathbb{F}_2^n$, таких, что $|C| = 2^{n-1}$. К сожалению, число $2^{2^{n-1}}$ уже при $n \geqslant 7$ очень велико для того, чтобы перебрать всевозможные варианты недостающих координатных булевых функций и проверить, является ли APN-функцией построенная взаимно однозначная функция. Поэтому, для того, чтобы оценить эффективность частичного перебора, необходимо найти количество тех булевых функций, которые дают именно APN-перестановку.*

3.3.2 Оценка числа координатных булевых функций для 2-в-1 функции специального вида

Для произвольного натурального k рассмотрим векторное пространство $\mathbb{F}_2^k$ и разобьем его на два равномощных непересекающихся подмножества $\mathbb{F}_2^k = V_1 \cup V_2$ следующим образом: пусть $V_1 = \{v \in \mathbb{F}_2^k \mid wt(v) \text{ — нечетное число}\}$ и

$V_2 = \{v \in \mathbb{F}_2^k \mid wt(v) -$ четное число$\}$. Рассмотрим произвольную взаимно однозначную функцию $F = (f_1, \ldots, f_n)$, где $n \in N$ и $n \geqslant k$. Зафиксируем k координатных функций $f_{i_1}, \ldots, f_{i_k}$ и разобьем векторное пространство $\mathbb{F}_2^n$ на два непересекающихся подмножества $\mathcal{F}_1^{i_1,\ldots,i_k}$ и $\mathcal{F}_2^{i_1,\ldots,i_k}$ следующим образом:

$$\mathcal{F}_j^{i_1,\ldots,i_k} = \{(f_1(x), \ldots, f_n(x)) \mid f_{i_1}(x), \ldots, f_{i_k}(x) \in V_j,\ x \in \mathbb{F}_2^n\}.$$

Пусть дано значение k, а также набор индексов $i_1, \ldots, i_k$ и индекс $j \notin \{i_1, \ldots, i_k\}$. Определим ассоциированную перестановку $F^\star$ следующим образом:

$$F^\star(x) = \begin{cases} F(x), & \text{если } F(x) \in \mathcal{F}_1^{i_1,\ldots,i_k}; \\ F(x) + e_j, & \text{если } F(x) \in \mathcal{F}_2^{i_1,\ldots,i_k}. \end{cases}$$

Для данной конструкции справедлива следущая теорема.

Теорема 4. *Перестановка F является APN-функцией тогда и только тогда, когда перестановка $F^\star$ является APN-функцией.*

Доказательство. Поскольку F — APN-функция, то для любого ненулевого вектора $a \in \mathbb{F}_2^n$ ее производная $D_aF(x) = F(x) + F(x+a)$ является 2-в-1 функцией. Зафиксируем произвольный вектор a' и рассмотрим вектор значений функции $D_{a'}F$. Он состоит из 2^{n-1} различных значений $B_{a'}F = \{b_1, \ldots, b_{2^{n-1}}\}$, каждое из которых встречается ровно 2 раза.

Рассмотрим перестановку $F^\star(x)$ и производную $D_{a'}F^\star$ для того же вектора a'. Без ограничения общности, для фиксированного аргумента x' возможны три случая:

1) $F(x') \in \mathcal{F}_1^{i_1,\ldots,i_k}$ и $F(x'+a') \in \mathcal{F}_1^{i_1,\ldots,i_k}$;
2) $F(x') \in \mathcal{F}_1^{i_1,\ldots,i_k}$ и $F(x'+a') \in \mathcal{F}_2^{i_1,\ldots,i_k}$;
3) $F(x') \in \mathcal{F}_2^{i_1,\ldots,i_k}$ и $F(x'+a') \in \mathcal{F}_2^{i_1,\ldots,i_k}$.

Рассмотрим первый случай. Поскольку оба значения $F(x')$ и $F(x'+a')$ лежат в $\mathcal{F}_1^{i_1,\ldots,i_k}$, то значение $D_{a'}F^\star(x') = D_{a'}F^\star(x'+a') = D_{a'}F(x') = D_{a'}F(x'+a')$ принадлежит $B_{a'}F$ и встречается два раза.

В третьем случае оба значения $F(x')$ и $F(x'+a')$ лежат в $\mathcal{F}_2^{i_1,\ldots,i_k}$. Тогда значение производной $D_{a'}F^\star(x')$ равно значению производной $D_{a'}F(x')$, поскольку $D_{a'}F^\star(x') = F^\star(x') + F^\star(x'+a') = F(x') + e_j + F(x'+a') + e_j = F(x') + F(x'+a')$. Заметим, что $D_{a'}F^\star(x')$ совпадает со значением $D_{a'}F^\star(x'+a')$, следовательно, оно принадлежит $B_{a'}F$ и встречается два раза.

Чтобы доказать, что перестановка $F^\star$ является APN-функцией, необходимо показать, что значение производной, получаемое во втором случае, отлично от

значений производной, получаемых в первом и третьем случаях, а также показать, что оно встретится в векторе значений функции $D_{a'}F^\star$ ровно два раза.

Докажем вторую часть необходимого условия. Поскольку $F(x')$ принадлежит $\mathcal{F}_1^{i_1,\dots,i_k}$, а $F(x'+a')$ принадлежит $\mathcal{F}_2^{i_1,\dots,i_k}$, то значение производной $D_{a'}F^\star(x')$ равно значению $D_{a'}F(x') + e_j$. Поскольку F — APN-функция, то значение $D_{a'}F(x')$ встречается ровно два раза, а значит, и $D_{a'}F^\star(x')$ встретится среди значений $D_{a'}F^\star$ ровно два раза.

Заметим, что для любой пары $v_1, w_1 \in V_1$ и любой пары $v_2, w_2 \in V_2$ выполнено $v_i + w_i \in V_2$, а для любой пары $v_1 \in V_1$, $v_2 \in V_2$ выполнено $v_1 + v_2 \in V_1$. Следовательно, по построению, множества $\mathcal{F}_1^{i_1,\dots,i_k}$ и $\mathcal{F}_2^{i_1,\dots,i_k}$ обладают аналогичными свойствами. А именно, для любой пары $v_1, w_1 \in \mathcal{F}_1^{i_1,\dots,i_k}$ и любой пары $v_2, w_2 \in \mathcal{F}_2^{i_1,\dots,i_k}$ выполнено $v_i + w_i \in \mathcal{F}_2^{i_1,\dots,i_k}$, а для любой пары $v_1 \in \mathcal{F}_1^{i_1,\dots,i_k}$, $v_2 \in \mathcal{F}_2^{i_1,\dots,i_k}$ выполнено $v_1 + v_2 \in \mathcal{F}_1^{i_1,\dots,i_k}$. Из этого следует, что значения производных в первом и третьем случае принадлежат $\mathcal{F}_2^{i_1,\dots,i_k}$, а значение производной во втором случае принадлежит $\mathcal{F}_1^{i_1,\dots,i_k}$. Следовательно, поскольку $\mathcal{F}_1^{i_1,\dots,i_k}$ и $\mathcal{F}_2^{i_1,\dots,i_k}$ не пересекаются, то производная $D_{a'}F^\star$ является 2-в-1 функцией. В силу произвольности выбора a' получаем, что производные функции $F^\star$ по всем направлениям являются 2-в-1 функциями, следовательно, $F^\star$ — APN-перестановка. □

Пусть S является 2-в-1 дифференциально 4-равномерной функцией из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$, принимающей значения из множества $\{0, \dots, 2^{n-1} - 1\}$, которая может быть представлена в виде $(n-1)$-подфункции $S = (s_1, \dots, s_{n-1})$. Обозначим через $n(S)$ число булевых функций s_n таких, что $H = (s_1, \dots, s_{n-1}, s_n)$ является APN-перестановкой.

Теорема 5. *Если* $n(S) \neq 0$, *то* $n(S) \geqslant 2^n$.

Доказательство. Из утверждения Теоремы 3 следует, что если $H = (s_1, \dots, s_{n-1}, s_n)$ является APN-перестановкой для некоторой булевой функции s_n, то ассоциированная перестановка $H^\star$ для некоторого набора индексов $i_1, \dots, i_k$ также является APN-функцией. Чтобы оценить число булевых функций s_n таких, что $H = (s_1, \dots, s_{n-1}, s_n)$ является APN-перестановкой, необходимо найти количество ассоциированных перестановок $H^\star$, имеющих общую $(n-1)$-подфункцию $S = (s_1, \dots, s_{n-1})$.

Для того, чтобы определить ассоциированную перестановку $H^\star$, в общем случае необходимо задать значение k, набор индексов $i_1, \dots, i_k$ и индекс

$j \notin \{i_1, \ldots, i_k\}$. Заметим, что перестановки H и $H^\star$ имеют общую $(n-1)$-подфункцию $S = (s_1, \ldots, s_{n-1})$ тогда и только тогда, когда $j = n$. Докажем, что каждой ассоциированной перестановке будет соответствовать свое число k и набор индексов $i_1, \ldots, i_k$, соответственно, для построения перестановки необходимо и достаточно будет задать лишь эти параметры. Для этого потребуется доказать, что ни для какого $k^* < k$ не найдется непересекающихся множеств V_1^*, V_2^* таких, что $\mathbb{F}_2^{k^*} = V_1^* \cup V_2^*$, и выполнено следующее свойство: для вектора длины k зафиксируем произвольные $t = k - k^*$ координат, тогда любой вектор $v^* \in V_i^*$ может быть получен выкалыванием этих t координат из некоторого вектора $v \in V_i$.

По построению, все векторы из $\mathbb{F}_2^k$ нечетного веса лежат в V_1, а значит, все векторы стандартного базиса e_j, где $j = 1, \ldots, k$, также лежат в V_1. Заметим, что нулевой вектор по построению лежит в V_2. Рассмотрим вектор e_j такой, что координата j встречается среди t фиксированных координат $i_1, \ldots, i_t$. После выкалывания координат $i_1, \ldots, i_t$ из e_j получается нулевой вектор, который принадлежит V_1^*, однако нулевой вектор также лежит и в V_2^*, поскольку он принадлежал V_2 до операции выкалывания. Поскольку для любого $k^* < k$ и любого $t = k - k^*$ такой вектор e_j найдется, то множества V_1^* и V_2^* всегда будут пересекаться для любых t и k^*.

Следовательно, для каждого k множества $\mathcal{F}_1^{i_1,\ldots,i_k}$ и $\mathcal{F}_2^{i_1,\ldots,i_k}$, полученные из таких V_1 и V_2, не совпадут ни с какими множествами $\mathcal{F}_1^{i_1,\ldots,i_{k^*}}$ и $\mathcal{F}_2^{i_1,\ldots,i_{k^*}}$, определенными для некоторого $k^* < k$. Это значит, что для каждой ассоциированной перестановки будет существовать единственное число k и единственный набор индексов $i_1, \ldots, i_k$, и для того, чтобы найти число возможных ассоциированных перестановок для APN перестановки H, нужно посчитать число возможных наборов координат $i_1, \ldots, i_k$ для каждого значения k, $k = 1, \ldots, n-1$. Их в точности $\sum_{j=1}^{n-1} C_{2^{n-1}}^j = 2^{n-1} - 1$.

Напомним, что прибавление аффинной функции не меняет свойства функции быть APN, следовательно, если $H = (s_1, \ldots, s_{n-1}, f)$ является APN-перестановкой, то и $G = (s_1, \ldots, s_{n-1}, f + \mathbf{1})$ также ей является. Заметим, что прибавление единицы к последней координате эквивалентно тому, что мы меняем местами множества V_1 и V_2 при построении $\mathcal{F}_1^{i_1,\ldots,i_k}$ и $\mathcal{F}_2^{i_1,\ldots,i_k}$. Вместе с исходной функцией H мы имеем 2^{n-1} APN-перестановок, а поскольку к последней координате каждой перестановки мы еще можем прибавить единицу, то всего получаем 2^n различных APN-перестановок, имеющих общую $(n-1)$-подфункцию $S = (s_1, \ldots, s_{n-1})$.

Таким образом, если существует хотя бы одна булева функция f такая, что $H = (s_1, \ldots, s_{n-1}, f)$ является APN-перестановкой и, следовательно, $n(S) \neq 0$, то $n(S) \geqslant 2^n$. □

С помощью компьютерных вычислений было установлено, что данная оценка является точной для $n = 3, 5$ и для всех рассмотренных спорадических примеров дифференциально 4-равномерных функций из $\mathcal{T}_n$ от 6 переменных.

В данной работе остаются открытыми несколько интересных вопросов. Пусть S является дифференциально 4-равномерной функцией из $\mathcal{T}_n$, может ли величина $n(S)$ быть равной нулю? Другими словами, из любой ли 2-в-1 дифференциально 4-равномерной функции из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$, принимающей значения из множества $\{0, \ldots, 2^{n-1} - 1\}$, можно получить APN-перестановку? Для всех рассмотренных примеров $n(S)$ не равнялась нулю. Напомним, что при $n = 4$ в $\mathcal{T}_n$ не существует дифференциально 4-равномерных функций, как не существует и самих APN-перестановок. Это позволяет предполагать, что проблема поиска взаимно однозначных APN-функций от четного числа переменных может быть сведена к поиску дифференциально 4-равномерных функций, которые, в свою очередь, если верна Гипотеза 2, все могут быть построены с помощью допустимых символьных последовательностей.

Понятия EA-эквивалентности и CCZ-эквивалентности очень важны, когда мы говорим о поиске новых функций, поскольку найти новую APN-перестановку от 6 переменных — это найти APN-перестановку, неэквивалентную APN-функции Диллона. Можно заметить, что утверждение Теоремы 4 задает отношение эквивалентности на множестве APN-перестановок. Как эта эквивалентность соотносится с уже известными отношениями эквивалентности? Так, мы проверили несколько пар ассоциированных APN-перестановок от 5 и 6 переменных, и все рассмотренные примеры являлись попарно CCZ-эквивалентными. Однако, конструкция ассоциированной перестановки позволяет предположить, что новое отношение эквивалентности в общем случае шире, чем EA-эквивалентность.

Глава 4

Симметрические свойства APN-функций

В силу сложности описания класса почти совершенно нелинейных функций естественно рассматривать свойства наиболее простых его представителей, таких, как функции с низкой алгебраической степенью, симметрические функции и т.д. Данная глава посвящена изучению симметрических свойств APN-функций. Исследуется возможность существования симметрических представителей среди APN-функций и доказываются верхние оценки числа координатных симметрических функций у APN-функции и координатных функций, инвариантных относительно циклического сдвига. Получена нижняя оценка числа различных значений APN-функции, доказываются верхние оценки мощности множества векторов, на которых APN-функция принимает одно и то же значение.

4.1 Симметрические представители класса APN-функций

Напомним, что *симметрической группой* S_n некоторого множества X из n элементов называется группа всех перестановок $\pi : X \to X$. Здесь и далее, результатом применения перестановки π к вектору $x = (x_1, \ldots, x_n)$ будем называть вектор $\pi(x) = (x_{\pi(1)}, \ldots, x_{\pi(n)})$. Напомним определение симметрической булевой функции. Булева функция от n переменных f — *симметрическая*, если для любой перестановки $\pi \in S_n$ для любых $x_1, \ldots, x_n$ выполнено $f(x_1, \ldots, x_n) = f(x_{\pi(1)}, \ldots, x_{\pi(n)})$.

Можно заметить, что значение симметрической булевой функции $f(x)$ зависит только от веса вектора x, следовательно, вектор значений и АНФ такой функции могут быть представлены в более компактном виде, что может быть полезно при аппаратной и программной реализации шифра.

Имеет место [9] следующее альтернативное определение APN-функции. Для векторной булевой функции F и произвольного вектора $a \neq 0$ определим множество $B_a(F) = \{F(x) + F(x+a) \mid x \in \mathbb{Z}_2^n\}$. Тогда F — APN-функция тогда и толь-

ко тогда, когда для любого ненулевого a выполнено $|B_a(F)| = 2^{n-1}$. Следующая теорема доказывает невозможность существования APN-функции, сохраняющей свои значения при произвольной перестановке переменных.

Теорема 6. *Пусть F — APN-функция от n переменных. Тогда не существует перестановки $\pi \in S_n$, отличной от тождественной, такой что $F(x) = F(\pi(x))$ для любого $x \in \mathbb{F}_2^n$.*

Доказательство. Предположим обратное. Пусть существует такая перестановка $\pi \in S_n$, что для любого x справедливо $F(x) = F(\pi(x))$, т.е. $F(x_1, \ldots, x_n) = F(x_{\pi(1)}, \ldots, x_{\pi(n)})$.

Докажем, что для любой перестановки π существует ненулевой вектор a, такой, что $F(\pi(x)+a) = F(\pi(x+a))$. Для этого достаточно выполнения равенства $\pi(x) + a = \pi(x + a)$.

Расписав подробней последнее условие, получаем $\pi(x) + a = (x_{\pi(1)} + a_1, \ldots, x_{\pi(n)} + a_n)$, $\pi(x + a) = (x_{\pi(1)} + a_{\pi(1)}, \ldots, x_{\pi(n)} + a_{\pi(n)})$, и, следовательно, справедлива следующая система уравнений:

$$\begin{cases} a_1 = a_{\pi(1)} \\ \quad \ldots \\ a_n = a_{\pi(n)} \end{cases}$$

В этой системе n уравнений и n неизвестных, и как минимум одно решение — вектор $a = (1, 1, \ldots, 1)$.

Заметим, что существует вектор x^*, такой, что $\pi(x^*) \neq x^*$ и $\pi(x^*) \neq x^* + a$, где $a = (1, 1, \ldots, 1)$. Действительно, случай $\pi(x^*) = x^* + a$ возможен только при условии $wt(x^*) = n/2$. Так как перестановка π отлична от тождественной, значит, хотя бы для одного индекса j выполнено $j \neq \pi(j)$, поэтому, если в векторе x^* выполнено $x_j \neq x_{\pi_j}$, то $\pi(x^*) \neq x^*$. Поэтому, в качестве вектора x^* можно выбрать любой вектор веса, отличного от $n/2$, в котором j-я и $\pi(j)$-я координаты различны.

Пусть $F(x^*)+F(x^*+a) = b^*$ для $a = (1, 1, \ldots, 1)$, где x^* — выбранный вектор. Тогда $F(\pi(x^*) + a) = F(\pi(x^* + a))$ и мы получаем противоречие с тем, что F — APN-функция, поскольку, тогда $F(\pi(x^*)) + F(\pi(x^*) + a) = F(\pi(x^*)) + F(\pi(x^* + a)) = F(x^*) + F(x^* + a) = b^*$, что невозможно, так как $\left|B_a(F)\right| = 2^{n-1}$. □

Напомним, что C_n^k — биномиальный коэффициент и $C_n^k = \frac{n!}{(n-k)!k!}$. В силу несуществования симметрической APN-функции, интересен вопрос о ее координатных булевых функциях — могут ли они быть симметрическими функциями? Следующая теорема дает ответ на этот вопрос.

Теорема 7. *Пусть F — APN-функция из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$, $F = (f_1, \ldots, f_n)$, где f_i — координатные булевы функции. Тогда, среди $f_1, \ldots, f_n$ не более $\lfloor n - \log_2 C_n^{\lfloor \frac{n-1}{2} \rfloor} \rfloor$ симметрических.*

Доказательство. Предположим обратное. Пусть у нас $\sigma(n)$ симметрических координатных функций $f_1, \ldots, f_{\sigma(n)}$ и выполнено $\sigma(n) > \lfloor n - \log_2 C_n^{\lfloor \frac{n-1}{2} \rfloor} \rfloor$, что эквивалентно $C_n^{\lfloor \frac{n-1}{2} \rfloor} > 2^{n-\sigma(n)}$. Для вектора из всех единиц рассмотрим следующую систему:

$$\begin{cases} f_1(x) + f_1(x+1) = b_1 \\ f_2(x) + f_2(x+1) = b_2 \\ \ldots \\ f_{\sigma(n)}(x) + f_{\sigma(n)}(x+1) = b_{\sigma(n)} \\ f_{\sigma(n)+1}(x) + f_{\sigma(n)+1}(x+1) = b_{\sigma(n)+1} \\ \ldots \\ f_n(x) + f_n(x+1) = b_n. \end{cases} \quad (1)$$

Рассмотрим произвольный вектор x веса $\lfloor \frac{n-1}{2} \rfloor$. Таких векторов ровно $C_n^{\lfloor \frac{n-1}{2} \rfloor}$. Заметим, что это максимальное количество векторов с одного слоя, таких что $wt(x) \neq wt(x+a)$, и для любых таких двух векторов x', x'' выполняется $f_i(x') + f_i(x'+a) = f_i(x'') + f_i(x''+a) = b_i$ где $i = 1, \ldots, \sigma(n)$. Возможных вариантов значения вектора $(b_{\sigma(n)+1}, \ldots, b_n)$ существует $2^{n-\sigma(n)}$, однако количество векторов веса $\lfloor \frac{n-1}{2} \rfloor$ больше, чем $2^{n-\sigma(n)}$, поэтому найдутся хотя бы два таких вектора x_1 и x_2 веса $\lfloor \frac{n-1}{2} \rfloor$, что $F_a^*(x_1) = (f_{\sigma(n)+1}(x_1) + f_{\sigma(n)+1}(x_1+a), \ldots, f_n(x_1) + f_n(x_1+a)) = (b_{\sigma(n)+1}, \ldots, b_n) = F_a^*(x_2)$. Следовательно, так как для этих двух векторов значения первых $\sigma(n)$ координатных функций совпадают ввиду их симметричности, то $F(x_1) + F(x_1+a) = b$ и $F(x_2) + F(x_2+a) = b$ для некоторых $x_1 \neq x_2$, таких, что $x_1 + a \neq x_2$, что противоречит тому, что F — APN-функция. □

Помимо симметрических булевых функций интерес в криптографии представляют также функции, которые сохраняют значения на всех циклических сдвигах координат вектора. Булева функция называется *инвариантной относительно циклического сдвига (rotation symmetric Boolean function — RotS*, см. [74]), если

$$f(x_1, x_2, \ldots, x_n) = f(x_2, \ldots, x_n, x_1) = \ldots = f(x_n, x_1, \ldots, x_{n-1})$$

для любого вектора x из $\mathbb{F}_2^n$. Следующее утверждение дает верхнюю оценку количества координатных RotS-функций у APN-функции.

Теорема 8. *Пусть F — APN-функция от n переменных, $F = (f_1, \ldots, f_n)$, где f_i — координатные булевы функции. Тогда, среди $f_1, \ldots, f_n$ не более $\lfloor n - \log_2 n \rfloor$ RotS-функций.*

Доказательство. От противного. Пусть $\rho(n)$ координатных функций являются инвариантными относительно циклического сдвига, $f_1, \ldots, f_{\rho(n)}$, и выполнено $\rho(n) > \lfloor n - \log_2 n \rfloor$, что эквивалентно $n > 2^{n-\rho(n)}$. По аналогии с предыдущим доказательством рассматриваем систему (1) и все векторы веса 1 — каждый из n таких векторов может быть получен с помощью циклического сдвига из любого другого. Возможных вариантов значения вектора $(b_{t+1}, \ldots, b_{\rho(n)})$ существует $2^{n-\rho(n)}$, однако количество векторов веса 1 больше, чем $2^{n-\rho(n)}$, поэтому существуют хотя бы два вектора x_1 и x_2, отличающиеся на некоторый сдвиг, такие, что $F_a^*(x_1) = (f_{\rho(n)+1}(x_1) + f_{\rho(n)+1}(x_1 + a), \ldots, f_n(x_1) + f_n(x_1 + a)) = (b_{\rho(n)+1}, \ldots, b_n) = F_a^*(x_2)$. Следовательно, $F(x_1) + F(x_1 + a) = b$ и $F(x_2) + F(x_2 + a) = b$ для некоторых $x_1 \neq x_2$, таких, что $x_1 + a \neq x_2$, и F не может быть APN-функцией.

□

4.2 Множество значений APN-функции

Ввиду несуществования симметрической APN-функции и строгих ограничений на число её симметрических координатных функций возникают естественные вопросы — насколько далек класс APN-функций от симметрических, и, следовательно, насколько разнообразно множество значений такой функции? В данном разделе исследуются эти вопросы.

4.2.1 Свойства множества значений APN-функции

Известно, что при нечетных n и при $n = 6$ существуют взаимно однозначные APN-функции, следовательно, максимально возможное число различных значений достигается на таких функциях, однако, при четных n в общем случае точные верхние оценки неизвестны. Следующее утверждение дает нижнюю оценку числа различных значений произвольной APN-функции.

Утверждение 6. *Любая APN-функция F от n переменных принимает не менее $\mu(n)$ различных значений, где*

$$\mu(n) = \frac{1 + \sqrt{2^{n+2} - 7}}{2}.$$

Доказательство. Так как F — APN-функция, то мощность множества $B_a(F)$ равна 2^{n-1}. Пусть $\mu(n)$ — мощность множества значений функции F. Заметим, что для того, чтобы выполнялось $|B_a(F)| = 2^{n-1}$, необходимо, чтобы $C^2_{\mu(n)} + 1 \geqslant 2^{n-1}$. Отсюда получаем:

$$\frac{\mu(n)!}{2!(\mu(n) - 2)!} + 1 \geqslant 2^{n-1};$$

$$\mu(n)(\mu(n) - 1) \geqslant 2^n - 2.$$

Решая квадратное неравенство, получаем оценку

$$\mu(n) \geqslant \frac{1 + \sqrt{2^{n+2} - 7}}{2}.$$

□

Пусть функция F принимает t различных значений $y_1, \ldots, y_t$. Определим множество $M_i = \{x \in \mathbb{F}_2^n \mid F(x) = y_i\}$. Через M_{max} будем обозначать максимальное по мощности множество M_i. Из Утверждения 6 естественно следует верхняя оценка мощности множества M_{max}.

Следствие 1. *Пусть F — APN-функция от n переменных. Тогда $|M_{max}| \leqslant 2^n - \mu(n) + 1$.*

Доказательство. Заметим, что поскольку у функции должно быть не менее $\mu(n)$ различных значений, то в векторе ее значений остается $2^n - \mu(n)$ произвольных векторов, которые уже не обязательно являются различными, поэтому возможный максимум количества совпадающих значений реализуется тогда, когда все эти $2^n - \mu(n)$ векторы совпадают с одним из $\mu(n)$ различных значений. □

К сожалению, эта оценка для достаточно больших n становится тривиальной, поэтому необходимо более тщательное исследование множеств M_i и их максимально возможной мощности.

4.2.2 Оценки числа одинаковых значений APN-функции

Для произвольной APN-функции и любого ее множества M_i справедливо следующее свойство.

Утверждение 7. *Пусть F — APN-функция. Тогда, для любого i, для любых попарно различных векторов v_1, v_2, v_3, v_4 из M_i выполняется $v_1 + v_2 + v_3 + v_4 \neq 0$. В частности, никакое аффинное подпространство L, $dim(L) \geqslant 2$, не может быть подмножеством M_i.*

Доказательство. Предположим обратное. Пусть для некоторого i найдутся четыре вектора v_1, v_2, v_3, v_4 из M_i, такие, что $v_1 + v_2 + v_3 + v_4 \neq 0$. Следовательно, $v_1 + v_2 = v_3 + v_4 = a$. Для вектора a рассмотрим множество $B_a(F)$. Для APN-функции выполняется $|B_a(F)| = 2^{n-1}$, но $F(v_1) + F(v_1 + a) = F(v_1) + F(v_2) = 0$ и $F(v_3) + F(v_3 + a) = F(v_3) + F(v_4) = 0$, а значит, мощность $B_a(F)$ меньше, чем 2^{n-1}. □

Из Утверждения 7 следует оценка мощности множества M_{max}.

Теорема 9. *Пусть F — произвольная APN-функция от n переменных. Тогда выполняется $|M_{max}| \leqslant \sqrt{2^{n+1} - 1} + 1$.*

Доказательство. Рассмотрим произвольное множество $M \subseteq \mathbb{F}_2^n$ такое, что сумма любых четырех различных векторов из M не равна нулю, и пусть m обозначает мощность множества M. Заметим, что для всех попарно различных векторов $x, y, x', y' \in M$ векторы $x + y$ и $x' + y'$ также различны, поскольку если $x + y = x' + y'$, то $x + y + x' + y' = 0$, что противоречит определению множества M.

Зафиксируем один из элементов множества M, скажем, x_1 и рассмотрим множество $M' = M \backslash \{x_1\}$. Существует $(m-1)(m-2)/2$ способов выбрать пару элементов из множества M', следовательно, для всех $x, y \in M'$, таких, что $x \neq y$, имеется $(m-1)(m-2)/2$ различных векторов $z = x_1 + x + y$, которые лежат в $\mathbb{F}_2^n \backslash M$. Таким образом, мы имеем оценку $m + (m-1)(m-2)/2 \leqslant 2^n$, что эквивалентно $m \leqslant \sqrt{2^{n+1} - 1} + 1$. Следовательно, в силу произвольности множества M выполнено $|M_{max}| \leqslant \sqrt{2^{n+1} - 1} + 1$.

□

Следующая таблица (см. Таблицу 4.1) содержит значения $\phi(n) = \lfloor\sqrt{2^{n+1}-1}+1\rfloor$ для $n \leqslant 16$.

Таблица 4.1: Значения $\phi(n) = \lfloor\sqrt{2^{n+1}-1}+1\rfloor$ для $n \leqslant 16$.

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\phi(n)$	3	4	6	8	12	16	23	32	46	64	91	128	182	256	363

С помощью свойств линейных пространств данная оценка может быть улучшена для $n \leqslant 6$.

Теорема 10. *Пусть F — APN-функция от n переменных, $n \leqslant 6$. Тогда мощность $|M_{max}|$ не превышает числа $\xi(n)$, где $\xi(n)$ принимает следующие значения:*

n	*2*	*3*	*4*	*5*	*6*
$\xi(n)$	*3*	*4*	*6*	*7*	*11*

Доказательство. Идея доказательства заключается в том, чтобы для каждого n найти максимально возможную мощность подмножества M векторов в $\mathbb{F}_2^n$, такого, что ни для каких четырех попарно различных векторов v_1, v_2, v_3, v_4 не выполнено $v_1 + v_2 + v_3 + v_4 = 0$. Мощность этого подмножества и будет верхней оценкой для $|M_{max}|$.

Для каждой размерности n мы всегда можем выбрать n линейно независимых векторов. Пусть, без ограничения общности, это вектора $e_1, \ldots, e_n$ с единицей в соответствующей координате.

• Для $n = 2$ доказательство тривиально — само $\mathbb{F}_2^n$ есть линейное пространство размерности 2, следовательно, все его четыре вектора входить в множество M_{max} не могут, но для любых трех векторов условие из Утверждения 7 выполнено, следовательно, $\xi(n) = 3$.

• Пусть $n = 3$. Рассмотрим все векторы в $\mathbb{F}_2^n$, разбив их в группы по весу:
$wt(v) = 0$: $\{0\}$;
$wt(v) = 1$: $\{e_1, e_2, e_3\}$;
$wt(v) = 2$: $\{e_1 + e_2, e_2 + e_3, e_1 + e_3\}$;
$wt(v) = 3$: $\{e_1 + e_2 + e_3\}$.

Опишем общий метод построения такого подмножества M_{max} для любого n. В M_{max} набираем все векторы веса 1 (как мы условились, без ограничения общности это произвольно выбранные векторы базиса). Далее, в каждой группе по весу удаляем векторы, которые с векторами внутри группы и базисными векторами образуют линейную комбинацию из четырех векторов, равную нулю. Затем

смотрим на выполнение условия уже для векторов между группами различного веса и удаляем те, которые ему не удовлетворяют. Оставшиеся векторы и образуют максимальное по мощности множество, свободное от векторов v_1, v_2, v_3, v_4 таких, что $v_1 + v_2 + v_3 + v_4 = 0$.

Рассмотрим группу, состоящую из таких векторов v, что $wt(v) = 2$. Вектор $e_1 + e_2$ не образует линейную комбинацию, равную нулю, с базисными векторами, поэтому можем его добавить в M_{max}. Заметим, что выбор здесь проводился без ограничения общности, мы могли добавить первым любой другой вектор веса 2. Рассмотрим следующие векторы $e_2 + e_3$ и $e_1 + e_3$ — в M_{max} уже есть вектор $e_1 + e_2$ и три базисных, и выполнено: $(e_2 + e_3) + (e_1 + e_2) + e_1 + e_3 = 0$, равно как и $(e_1 + e_3) + (e_1 + e_2) + e_2 + e_3 = 0$, поэтому из векторов веса 2 только один может попасть в M_{max}. Вектор нулевого веса не образует с базисными векторами линейную комбинацию, равную нулю. В группе $wt(v) = 3$ единственный вектор $e_1+e_2+e_3$ в сумме с тремя базисными векторами дает 0, поэтому он тоже удаляется. Итого $M_{max} = \{0, e_1, e_2, e_3, e_1 + e_2\}$, однако $e_1 + e_2 + (e_1 + e_2) + 0 = 0$, поэтому нулевой вектор удаляется из M_{max}, следовательно, $|M_{max}| \leq 4$.

• Пусть $n = 4$. Группы векторов соответствующие:
$wt(v) = 0$: $\{0\}$;
$wt(v) = 1$: $\{e_1, e_2, e_3, e_4\}$;
$wt(v) = 2$: $\{e_1 + e_2, e_1 + e_3, e_1 + e_4, e_2 + e_3, e_2 + e_4, e_3 + e_4\}$;
$wt(v) = 3$: $\{e_1 + e_2 + e_3, e_1 + e_2 + e_4, e_1 + e_3 + e_4, e_2 + e_3 + e_4\}$;
$wt(v) = 4$: $\{e_1 + e_2 + e_3 + e_4\}$.

Снова в M_{max} помещаем базисные векторы, нулевой вектор и рассматриваем оставшиеся группы по весу. В группе $wt(v) = 2$ без ограничения общности рассматриваем вектор $e_1 + e_2$, он не противоречит набору базисных векторов, поэтому помещаем его в M_{max}. Тогда векторы $e_1 + e_3$ и $e_1 + e_4$ должны быть удалены, поскольку $(e_1+e_2)+(e_1+e_3)+e_2+e_3 = 0$ и $(e_1+e_2)+(e_1+e_4)+e_2+e_4 = 0$. Следующие два вектора $(e_2 + e_3)$ и $(e_2 + e_4)$ удаляются поскольку для них выполнено $(e_1 + e_2) + (e_2 + e_3) + e_1 + e_3 = 0$ и $(e_1 + e_2) + (e_2 + e_4) + e_1 + e_4 = 0$. Вектор $e_3 + e_4$ не противоречит базисным векторам и вектору $e_1 + e_2$, поэтому мы добавляем его в M_{max}. Таким образом, на данном этапе $M_{max} = \{0, e_1, e_2, e_3, e_4, e_1 + e_2, e_3 + e_4\}$.

Теперь рассматриваем группу $wt(v) = 3$. Заметим, что для любого вектора веса три всегда найдутся три базисных вектора, которые в сумме с ним дадут нулевой вектор, поэтому ни один вектор из этой группы не может попасть в M_{max}. В последней группе всего один вектор $e_1+e_2+e_3+e_4$ и он не противоречит базисным векторам, поэтому добавляем его в M_{max}.

Теперь M_{max} состоит из следующих векторов: $0, e_1, e_2, e_3, e_4, e_1+e_2, e_3+e_4, e_1+e_2+e_3+e_4$. Однако, заметим, что $(e_1+e_2+e_3+e_4)+(e_1+e_2)+e_3+e_4=0$ и $(e_1+e_2+e_3+e_4)+(e_3+e_4)+e_1+e_2=0$, поэтому вектор $e_1+e_2+e_3+e_4$ не может принадлежать M_{max} (мы удаляем его, поскольку иначе придется удалить оба вектора e_1+e_2 и e_3+e_4, что противоречит максимальности множества). Тем не менее нулевой вектор придется удалить, поскольку $0+e_1+e_2+(e_1+e_2)=0$ и $0+e_3+e_4+(e_3+e_4)=0$, следовательно, $|M_{max}| \leq 6$.

• Для $n=5$ имеем следующие группы векторов:

$wt(v)=0$: $\{0\}$;

$wt(v)=1$: $\{e_1, e_2, e_3, e_4, e_5\}$;

$wt(v)=2$: $\{e_1+e_2, e_1+e_3, e_1+e_4, e_1+e_5, e_2+e_3, e_2+e_4, e_2+e_5, e_3+e_4, e_3+e_5, e_4+e_5\}$;

$wt(v)=3$: $\{e_1+e_2+e_3, e_1+e_2+e_4, e_1+e_2+e_5, e_1+e_3+e_4, e_1+e_3+e_5, e_1+e_4+e_5, e_2+e_3+e_4, e_2+e_3+e_5, e_2+e_4+e_5, e_3+e_4+e_5\}$;

$wt(v)=4$: $\{e_1+e_2+e_3+e_4, e_1+e_2+e_3+e_5, e_1+e_2+e_4+e_5, e_1+e_3+e_4+e_5, e_2+e_3+e_4+e_5\}$;

$wt(v)=5$: $\{e_1+e_2+e_3+e_4+e_5\}$.

Аналогично, нулевой вектор и вектор максимального веса единственны в своей группе и не образуют с базисными векторами линейную комбинацию, равную нулю, поэтому попадают в M_{max}. Заметим, что ни один вектор веса 3 не может находиться в M_{max}.

Рассмотрим группу $wt(v)=2$. Как мы видели раньше, из этой группы в M_{max} могут попадать только те представители, которые не пересекаются по составляющим базисным векторам, поскольку $(e_i+e_j)+(e_i+e_k)+e_k+e_j=0$, поэтому из второй группы без ограничения общности мы берем векторы e_1+e_2 и e_3+e_4. В группе $wt(v)=4$ можем без противоречий с базисными векторами взять любой вектор, например $e_1+e_2+e_3+e_4$, однако любой другой вектор пересекается с ним по трем составляющим базисным векторам, поэтому в силу свойства $(e_{j_1}+e_{j_2}+e_{j_3}+e_{j_4})+(e_{j_1}+e_{j_2}+e_{j_3}+e_{j_5})+e_{j_4}+e_{j_5}=0$ данный вектор единственный из группы веса 4, который может попасть в M_{max}.

На данном этапе M_{max} состоит из следующих векторов: $\{0, e_1, e_2, e_3, e_4, e_5, e_1+e_2, e_3+e_4, e_1+e_2+e_3+e_4, e_1+e_2+e_3+e_4+e_5\}$, однако $(e_1+e_2+e_3+e_4+e_5)+(e_1+e_2)+(e_3+e_4)+e_5=0$ и $(e_1+e_2+e_3+e_4+e_5)+(e_1+e_2+e_3+e_4)+e_4+0=0$, поэтому вектор веса 5 удаляется из M_{max}. Аналогично $(e_1+e_2)+e_1+e_2+0=0$ и $(e_3+e_4)+e_3+e_4+0=0$, поэтому удаляется нулевой вектор. Для вектора $e_1+e_2+e_3+e_4$ выполнено $(e_1+e_2+e_3+e_4)+(e_1+e_2)+e_3+e_4=0$, поэтому

в M_{max} остаются только базисные вектора и два вектора веса 2, следовательно для $n = 5$ справедливо $|M_{max}| \leq 7$.

• Для $n = 6$ имеем следующие группы векторов:

$wt(v) = 0$: $\{0\}$;

$wt(v) = 1$: $\{e_1, e_2, e_3, e_4, e_5, e_6\}$;

$wt(v) = 2$: $\{e_1 + e_2, e_1 + e_3, e_1 + e_4, e_1 + e_5, e_1 + e_6, e_2 + e_3, e_2 + e_4, e_2 + e_5, e_2 + e_6, e_3 + e_4, e_3 + e_5, e_3 + e_6, e_4 + e_5, e_4 + e_6, e_5 + e_6\}$;

$wt(v) = 3$: $\{e_1+e_2+e_3, e_1+e_2+e_4, e_1+e_2+e_5, e_1+e_2+e_6, e_1+e_3+e_4, e_1+e_3+e_5, e_1+e_3+e_6, e_1+e_4+e_5, e_1+e_4+e_6, e_1+e_5+e_6, e_2+e_3+e_4, e_2+e_3+e_5, e_2+e_3+e_6, e_2+e_4+e_5, e_2+e_4+e_6, e_2+e_5+e_6, e_3+e_4+e_5, e_3+e_4+e_6, e_3+e_5+e_6, e_4+e_5+e_6\}$;

$wt(v) = 4$: $\{e_1+e_2+e_3+e_4, e_1+e_2+e_3+e_5, e_1+e_2+e_3+e_6, e_1+e_2+e_4+e_5, e_1+e_2+e_4+e_6, e_1+e_2+e_5+e_6, e_1+e_3+e_4+e_5, e_1+e_3+e_4+e_6, e_1+e_3+e_5+e_6, e_1+e_4+e_5+e_6 e_2+e_3+e_4+e_5, e_2+e_3+e_4+e_6, e_2+e_3+e_5+e_6, e_2+e_4+e_5+e_6, e_3+e_4+e_5+e_6\}$;

$wt(v) = 5$: $\{e_1 + e_2 + e_3 + e_4 + e_5, e_1 + e_2 + e_3 + e_4 + e_6, e_1 + e_2 + e_3 + e_5 + e_6, e_1 + e_2 + e_4 + e_5 + e_6, e_1 + e_3 + e_4 + e_5 + e_6, e_2 + e_3 + e_4 + e_5 + e_6\}$;

$wt(v) = 6$: $\{e_1 + e_2 + e_3 + e_4 + e_5 + e_6\}$.

Как и в предыдущих размерностях, базисные векторы и нулевой вектор автоматически помещаются в M_{max}, а векторы веса три удаляются. Векторы веса два, имеющие пересечения по ненулевым координатам, не могут быть одновременно помещены в M_{max}, поэтому, без ограничения общности в M_{max} помещаются векторы $e_1 + e_2$,$e_3 + e_4$ и $e_5 + e_6$.

Рассмотрим группу $wt(v) = 4$. Без ограничения общности добавляем вектор $e_1+e_2+e_3+e_4$. Векторы, которые пересекаются с ним по трем базисным векторам не могут попасть в M_{max}, поскольку $(e_{j_1} + e_{j_2} + e_{j_3} + e_{j_4}) + (e_{j_1} + e_{j_2} + e_{j_3} + e_{j_5}) + e_{j_4} + e_{j_5} = 0$, значит удаляются векторы $e_1 + e_2 + e_3 + e_5$, $e_1 + e_2 + e_3 + e_6$, $e_1+e_2+e_4+e_5$, $e_1+e_2+e_4+e_6$, $e_1+e_3+e_4+e_5$, $e_1+e_3+e_4+e_6$, $e_2+e_3+e_4+e_5$, $e_2 + e_3 + e_4 + e_6$. Заметим, что количество удаленных векторов не зависит от выбора первого вектора из группы, поэтому такое удаление корректно.

В группе $wt(v) = 5$ можно взять только один вектор, поскольку все векторы в этой группе пересекаются друг с другом по четырем базисным векторам, а значит для любой пары из $wt(v) = 5$ найдутся два базисных вектора, сумма с которыми даст 0. Поэтому без ограничения общности берем вектор $e_1+e_2+e_3+e_4 + e_5$. Единственный вектор веса 6 также оставляем.

На следующем этапе из M_{max} удаляем вектор $e_1+e_2+e_3+e_4+e_5+e_6$, поскольку в сумме с любым из векторов веса 4 и двумя базисными он даст 0. Вектор $e_1 + e_2 + e_3 + e_4 + e_5$ также будет удален, поскольку $(e_1 + e_2 + e_3 + e_4 + e_5) + (e_1 + e_2)+(e_3+e_4)+e_5 = 0$. Нулевой вектор также следует удалить для максимальности

искомого множества, поскольку $(e_1 + e_2 + e_3 + e_4) + (e_1 + e_2) + (e_3 + e_4) + 0 = (e_3+e_4+e_5+e_6)+(e_3+e_4)+(e_5+e_6)+0 = 0$. После удаления в $wt(v) = 4$ остались следующие векторы: $e_1+e_2+e_3+e_4$, $e_1+e_2+e_5+e_6$, $e_1+e_3+e_5+e_6$, $e_1+e_4+e_5+e_6$, $e_2+e_3+e_5+e_6$, $e_2+e_4+e_5+e_6$, $e_3+e_4+e_5+e_6$, однако, вместе с векторами веса 2 они не могут попасть в M_{max}, поскольку все они содержат либо сумму $e_1 + e_2$, либо $e_5 + e_6$, а значит с двумя базисными векторами всегда найдется сумма четырех векторов, равная нулю. Необходимо понять, удаление каких векторов даст максимально возможную мощность текущего M_{max} — векторов веса 2 или векторов веса 4. Заметим, что из семи векторов веса 4 есть три комбинации, дающие нам 0. Это суммы $(e_1+e_3+e_5+e_6)+(e_1+e_4+e_5+e_6)+(e_2+e_3+e_5+e_6)+(e_2+e_4+e_5+e_6) = 0$, $(e_1+e_2+e_5+e_6)+(e_1+e_4+e_5+e_6)+(e_2+e_3+e_5+e_6)+(e_3+e_4+e_5+e_6) = 0$, $(e_1+e_2+e_5+e_6)+(e_1+e_3+e_5+e_6)+(e_2+e_4+e_5+e_6)+(e_3+e_4+e_5+e_6) = 0$, каждые две комбинации пересекаются по двум различным векторам, поэтому недостаточно будет удалить только один вектор, чтобы избежать пересечения, придется удалить два, например, без ограничения общности, шестой и седьмой векторы. Запишем оставшееся множество векторов в виде матрицы, где строки и есть имеющиеся векторы:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Как можно заметить, сумма никаких четырех строк не равна нулю, поэтому следует удалить три вектора веса 2. Следовательно, в M_{max} остались только базисные векторы и пять векторов веса 4, описанных выше, и $|M_{max}| \leq 11$. □

На следующих функциях оценка $\xi(n)$ достигается:

$n = 2$, $F =$ (0 0 0 1);

$n = 3$, $F =$ (0 2 2 2 2 3 6 5);

$n = 5$, $F =$ (0 0 0 1 0 2 4 8 0 3 6 12 7 16 25 23 0 7 3 22 28 19 9 0 19 8 15 28 21 9 29 2).

Также для следующей функции достижима оценка $\xi(n) - 1$:

$n = 4$, $F =$(0 0 0 1 0 2 4 7 0 4 6 3 8 14 10 13).

Напомним, что вектор значений APN-функции здесь приводится в лексикографическом порядке аргумента функции.

Стоит отметить интересное свойство множеств M_i для APN-функций Касами и Голда. Напомним, что функции вида $F(x) = x^d$ над конечным полем $GF(2^n)$ называются мономиальными. Если $d = 2^t + 1$ и $(t, n) = 1$, то мономиальная функция называется *функцией Голда*, а если $d = 2^{2t} - 2^t + 1$ и $(t, n) = 1$, то она называется *функцией Касами*.

Для любого i кроме нуля, мощность M_i при четных значениях n равна 3, а число различных значений функции, соответственно $\frac{2^n-1}{3}$. Объяснение данного факта следует непосредственно из самой конструкции. Если рассмотреть следующие элементы поля $GF(2^n)$: $x = \alpha^k$, $x = \alpha^{k+\frac{2^n-1}{3}}$ и $x = \alpha^{k+2\frac{2^n-1}{3}}$, то можно заметить, что значение функции F на всех трех значениях переменной совпадает. Действительно, если F — функция Голда, то $F(\alpha^{k+\frac{2^n-1}{3}}) = (\alpha^{k+\frac{2^n-1}{3}})^{2^i+1} = \alpha^{k(2^i+1)+(2^n-1)\frac{2^i+1}{3}} = \alpha^{k(2^i+1)} = F(\alpha^k) = F(\alpha^{k+2\frac{2^n-1}{3}})$, поскольку $(i, n) = 1$, следовательно, i нечетно и $2^i + 1$ делится на 3, а по свойствам $GF(2^n)$ для любого x выполнено $x^{2^n-1} = 1$. Аналогично и для функций Касами, поскольку $2^{2i} - 2^i + 1$ также делится на 3 для любых нечетных i.

Глава 5

О представлении S-блоков при реализации в блочных шифрах

В данной главе рассматривается метод специального разбиения S-блоков (векторных булевых функций) для защиты аппаратного исполнения алгоритма от атак по сторонним каналам. Известно, что достаточно найти равномерное разбиение только для представителя класса аффинной эквивалентности — тогда существует преобразование, строящее разбиение для всех остальных S-блоков из класса. В работе [13] для трех из четырех классов аффинной эквивалентности взаимно однозначных S-блоков 3×3 были найдены разбиения, удовлетворяющие определенным требованиям, но большой перебор не позволил найти разбиение для четвертого класса $\mathcal{Q}_3^3$, поэтому вопрос о существовании равномерного разбиения для таких S-блоков оставался открытым. В данной главе доказывается, что не существует равномерного разбиения для класса $\mathcal{Q}_3^3$. Предлагается метод реализации S-блока в виде композиции нескольких S-блоков, для каждого из которых существует требуемое равномерное разбиение.

5.1 Предварительные сведения

Многие криптографические алгоритмы уязвимы к так называемым атакам по сторонним каналам, направленным на слабости в практической реализации алгоритма. Криптоаналитик изучает специфические для данной реализации параметры, например, такие, как потребляемая мощность, время выполнения операций, электромагнитное излучение. Сравнивая их на разных входных данных, и набрав некую статистику, он может получить информацию о секретном ключе, выполняемых в устройстве операциях и их параметрах.

Разностная атака по мощности (differential power attack — DPA) является одной из самых эффективных атак по сторонним каналам. Этот вид криптоанализа

сравнивает разности потребляемой мощности и промежуточных вычислений алгоритма за некоторый временной интервал в зависимости от входных данных. В качестве мер противодействия используются методы, маскирующие входные данные так, чтобы вычисления не зависели от них в явном виде. Однако, аппаратные реализации криптографических алгоритмов сложно защитить от разностной атаки по мощности, поскольку во время исполнения алгоритма возникают случайные сбои и неполадки аппаратуры. Одним из преимуществ метода *пороговой реализации*, предложенного в [62], является то, что он не привязан к конкретной аппаратной реализации, защищен от случайных сбоев, а также позволяет [63], [64] сохранять компактность аппаратного устройства. Данный метод представляет собой специальное разбиение S-блоков, удовлетворяющее некоторым свойствам, в частности, свойству равномерности.

Показано [13], что для всех S-блоков 3×3 и 4×4 существует равномерное разбиение на 3, 4 или 5 частей. Метод пороговой реализации также был использован для таких криптографических алгоритмов, как PRESENT [76], AES [14], [61], KECCAK [8], [11] и FIDES [12].

5.1.1 Равномерное разбиение S-блока

Рассмотрим векторную функцию $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Напомним, что данную функцию можно представить в виде $S = (f_1(x), \ldots, f_n(x))$, где $f_1, \ldots, f_n$ — координатные булевы функции от n переменных. Пусть $x = (x_1, \ldots, x_n)$, где x_i принимает значения из $\mathbb{F}_2$. Для некоторого натурального r представим каждую переменную x_i в виде суммы r новых булевых переменных $x_{i_1}, \ldots, x_{i_r}$, где первые $r-1$ переменных независимы и выбираются случайным образом, а переменная x_{i_r} подбирается так, что справедливо:

$$x_i = \sum_{j=1}^{r} x_{ij}.$$

Пусть $v = (x_{11}, \ldots, x_{nr})$. Представим функцию S в виде суммы r векторных функций:

$$S(x) = \sum_{j=1}^{r} S_j(v),$$

где $S_i : \mathbb{F}_2^{nr} \to \mathbb{F}_2^n$. Набор из r векторных функций $S_1, \ldots, S_r$ называется *разбиением* S-блока S *на* r *частей*. Введем следующие условия для разбиения:

1. *Неполнота*: для каждого $j = 1, \ldots, r$ функция S_j не должна зависеть от переменных x_{ij}, $i = 1, \ldots, n$.

2. *Взаимная однозначность*: функция $S^* : \mathbb{F}_2^{nr} \to \mathbb{F}_2^{nr}$, где $S^* = (S_1, \ldots, S_r)$, является взаимно однозначной.

Разбиение, удовлетворяющее этим двум условиям, называется *равномерным* разбиением S-блока на r частей. Примеры разбиений S-блоков приводятся далее в Разделе 5.1.3.

5.1.2 Классы эквивалентности S-блоков 3×3 и 4×4

Напомним, что функции F и G называются *расширенно аффинно эквивалентными (EA-эквивалентными)*, если $F = A_1 \circ G \circ A_2$, где A_1, A_2 — невырожденные аффинные преобразования над $\mathbb{F}_2^n$. Данное отношение эквивалентности разбивает все множество взаимно однозначных S-блоков на непересекающиеся классы. Ниже перечислены представители классов эквивалентности (см. [16]) для взаимно однозначных S-блоков 3×3:

Класс	Представитель	Вектор значений
$\mathcal{A}_1^3$	(x, y, z)	(0 1 2 3 4 5 6 7)
$\mathcal{Q}_1^3$	$(x, y, xy + z)$	(0 1 2 3 4 5 7 6)
$\mathcal{Q}_2^3$	$(x, y + xz, z + xy + xz)$	(0 1 2 3 4 6 7 5)
$\mathcal{Q}_3^3$	$(xy + xz + yz, x + y + xy + yz, x + z + yz)$	(0 1 2 4 3 6 7 5)

В классе $\mathcal{A}_1^3$ лежат S-блоки, содержащие только аффинные координатные функции. Его представитель — (x, y, z) является тождественной перестановкой. Представители остальных классов, $\mathcal{Q}_1^3$, $\mathcal{Q}_2^3$, $\mathcal{Q}_3^3$, содержат также квадратичные координатные функции. Необходимо отметить, что степень координатной булевой функции во взаимно однозначных S-блоках не превышает двух.

Утверждение 8. *[13] Если для некоторой векторной функции существует равномерное разбиение, то такое разбиение существует для любой аффинно эквивалентной ей функции.*

Для S-блоков 4×4 существует 302 класса эквивалентности [16]. Один класс аффинных, 6 классов квадратичных и 295 классов кубических функций. Кроме того, в [13] найдено преобразование, которое ставит в соответствие трем классам S-блоков 3×3 три класса S-блоков 4×4. Рассмотрим S-блок S из $\mathbb{F}_2^3$ в $\mathbb{F}_2^3$, и трансформируем его в $\widehat{S}$ следующим образом: Если $S(w, v, u) = (y_1, y_2, y_3)$, то $\widehat{S}(x, w, v, u) = (y_1, y_2, y_3, x)$. Такое преобразование отображает классы $\mathcal{Q}_1^3$, $\mathcal{Q}_2^3$ и $\mathcal{Q}_3^3$ в классы $\mathcal{Q}_4^4$, $\mathcal{Q}_{12}^4$ и $\mathcal{Q}_{300}^4$ соответственно. Благодаря этому можно, зная равномерное разбиение для S-блока 3×3, получить равномерное разбиение и

для соответствующего класса S-блоков 4×4 , и наоборот, если равномерного разбиения для представителя класса не существует, то и для представителей соответствующего ему класса также нет равномерного разбиения.

5.1.3 Непосредственное разбиение

Предположим, мы хотим построить равномерное разбиение для функции $S = (f, g, h)$. В [13] был предложен следующий метод разбиения булевых функций. Пусть $f : \mathbb{F}_2^3 \to \mathbb{F}_2$, где $f = f(x, y, z)$. Построить разбиение и добиться выполнения условия неполноты нетрудно — представим каждую булеву переменную в виде суммы трех:

$$x = \sum_{i=1}^{3} x_i,\ y = \sum_{i=1}^{3} y_i,\ z = \sum_{i=1}^{3} z_i.$$

Представим функцию f как сумму трех булевых функций:

$$f_1(v) + f_2(v) + f_3(v) = f(x, y, z) = f(x_1 + x_2 + x_3, y_1 + y_2 + y_3, z_1 + z_2 + z_3).$$

Чтобы разбиение удовлетворяло первому из требований — условию неполноты, необходимо распределить переменные так, чтобы f_j не зависела от переменных с индексом j. Для этого отнесем к f_1 линейные и квадратичные члены с индексом 2, а также квадратичные члены с индексами 2 и 3, к f_2 линейные и квадратичные с индексом 2 и квадратичные с индексами 3 и 1, а оставшиеся члены отнесем к f_3. Например, для функции $f = x + yz$ получаем:

$f_1 + f_2 + f_3 = f(x_1 + x_2 + x_3, y_1 + y_2 + y_3, z_1 + z_2 + z_3) = x_1 + x_2 + x_3 + (y_1 + y_2 + y_3)(z_1 + z_2 + z_3)$ Раскрываем скобки и распределяем переменные по функциям $f_1(v)$, $f_2(v)$ и $f_3(v)$:

$$f_1(v) = x_2 + y_2z_2 + y_2z_3 + y_3z_2;$$
$$f_2(v) = x_3 + y_3z_3 + y_3z_1 + y_1z_3;$$
$$f_3(v) = x_1 + y_1z_1 + y_1z_2 + y_2z_1.$$

Разбивая таким образом каждую булеву функцию, получаем разбиение векторной функции $S = (f, g, h)$. Нужно заметить, что свойство взаимной однозначности при таком разбиении может не выполняться и требует отдельной проверки. Данный метод (назовем его методом *непосредственного разбиения*) обобщается и для случая большего числа переменных. Полученное этим методом разбиение для всех S-блоков класса $\mathcal{Q}_1^3$ является равномерным, но для классов $\mathcal{Q}_2^3$ и $\mathcal{Q}_3^3$ второе условие не выполняется.

5.1.4 Корректирующие слагаемые

Для того, чтобы достигнуть взаимной однозначности разбиения векторной функции, авторы [13] используют пары специальных *корректирующих слагаемых* для изменения функции таким образом, чтобы по-прежнему выполнялось условие 1. Так как при сложении всех функций одно корректирующее слагаемое из пары аннулирует другое, то по-прежнему $S(x) = \sum_{j=1}^{r} S_j(v)$. Для сохранения условия неполноты могут использоваться только слагаемые вида x_i или $x_i y_i$ в функциях с индексом j, $j \neq i$, для $i = 1, \ldots, n$. Комбинируя различные корректирующие слагаемые, можно получить всевозможные разбиения для данного S-блока, удовлетворяющие условию 1.

Для S-блока 3×3 существует $3(3+C_3^2)$ различных корректирующих слагаемых и три функции f, g и h для их размещения. Таким образом, всевозможных комбинаций корректирующих слагаемых для S-блока 3×3 существует $2^{9(3+C_3^2)} = 2^{54}$. Заметим, что данное число слишком велико для того, чтобы полным перебором найти необходимую комбинацию или доказать, что ее не существует.

Рассмотрим пример разбиения S-блока $(x, y + xz, z + xy + xz)$ из $\mathcal{Q}_2^3$:

$S_1(v) = (x_2, y_2 + x_2z_2 + x_2z_3 + x_3z_2, z_2 + x_2y_2 + x_2y_3 + x_3y_2 + x_2z_2 + x_2z_3 + x_3z_2)$,

$S_2(v) = (x_3, y_3 + x_3z_3 + x_1z_3 + x_3z_1, z_3 + x_3y_3 + x_1y_3 + x_3y_1 + x_3z_3 + x_1z_3 + x_3z_1)$,

$S_3(v) = (x_1, y_1 + x_1z_1 + x_1z_2 + x_2z_1, z_1 + x_1y_1 + x_1y_2 + x_2y_1 + x_1z_1 + x_1z_2 + x_2z_1)$.

Оно не является равномерным, так как при проверке не выполняется свойство взаимной однозначности. Рассмотрим этот же S-блок и его разбиение после добавления некой комбинации корректирующих слагаемых (они выделены подчеркиванием).

$S_1\prime(v) = (x_2, y_2 + x_2z_2 + x_2z_3 + x_3z_2 + \underline{z_2}, z_2 + x_2y_2 + x_2y_3 + x_3y_2 + x_2z_2 + x_2z_3 + x_3z_2 + \underline{y_3} + \underline{z_2})$,

$S_2\prime(v) = (x_3, y_3 + x_3z_3 + x_1z_3 + x_3z_1 + \underline{z_1}, z_3 + x_3y_3 + x_1y_3 + x_3y_1 + x_3z_3 + x_1z_3 + x_3z_1 + \underline{y_3} + \underline{z_1})$,

$S_3\prime(v) = (x_1, y_1 + x_1z_1 + x_1z_2 + x_2z_1 + \underline{z_1} + \underline{z_2}, z_1 + x_1y_1 + x_1y_2 + x_2y_1 + x_1z_1 + x_1z_2 + x_2z_1 + \underline{z_1} + \underline{z_2})$.

Данное разбиение, в свою очередь, уже является равномерным.

5.1.5 Открытые вопросы

При использовании корректирующих слагаемых в [13] были найдены разбиения S-блоков из класса $\mathcal{Q}_2^3$, являющиеся равномерными. Но для класса $\mathcal{Q}_3^3$ равномерное разбиение так и не было найдено, а большой перебор комбинаций корректирующих слагаемых делает поиск трудным, поэтому в [13] авторы сфор-

мулировали открытый вопрос о том, существует ли для класса $\mathcal{Q}_3^3$ разбиение, являющееся равномерным. Соответственно, такой же вопрос стоит и для класса $\mathcal{Q}_{300}^4$.

5.2 Поиск равномерного разбиения

В данном разделе предлагается оптимизация перебора корректирующих слагаемых для некоторого непосредственного разбиения S-блока. Вводится понятие корректирующей функции и доказывается теорема о необходимом и достаточном условии взаимной однозначности ее суммы с исходным S-блоком. С помощью данной теоремы значительно сокращается полный перебор, в результате чего доказывается, что для рассматриваемого класса $\mathcal{Q}_3^3$ аффинной эквивалентности не существует равномерного разбиения. Ввиду его несуществования предлагается реализация S-блока в виде композиции нескольких S-блоков, для которых равномерное разбиение уже существует.

5.2.1 Оптимизация полного перебора корректирующих слагаемых

Рассмотрим, если оно существует, равномерное разбиение для некоторого S-блока $n \times n$. Свойство взаимной однозначности для равномерного разбиения равносильно тому, что векторная функция $S^* : \mathbb{F}_2^{nr} \to \mathbb{F}_2^{nr}, S^* = (S_1, \ldots, S_r)$ является сбалансированной. Рассмотрим некоторые свойства сбалансированных векторных функций.

Пусть $F = (f_1, \ldots, f_n)$ — векторная функция из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$. Легко заметить, что функция F является взаимно однозначной тогда и только тогда, когда для любого k, где $1 \leqslant k \leqslant n$, и для любого набора индексов $i_1, \ldots, i_k$, где $1 \leqslant i_1 \leqslant \ldots \leqslant i_k \leqslant n$, векторная функция $F_{i_1,\ldots,i_k} = (f_{i_1}, \ldots, f_{i_k})$ уравновешена.

Пусть $\mathbf{F} = (f_{11}, \ldots, f_{n1}, \ldots, f_{1s}, \ldots, f_{ns})$ — непосредственное разбиение функции F на s частей $F_i = (f_{1i}, \ldots, f_{ni})$. Будем говорить, что функция $\mathbf{C_F} = (c_{11}, \ldots, c_{n1}, \ldots, c_{1s}, \ldots, c_{ns})$, где $c_{ij} : \mathbb{F}_2^{ns} \to \mathbb{F}_2$ — корректирующие слагаемые, называется корректирующей функцией для $\mathbf{F}$, если функция $\mathbf{F} + \mathbf{C_F}$ обладает следующими свойствами:

1. $f_i = \sum_{j=1}^{r}(f_{ij} + c_{ij})$;

2. $f_{ij} + c_{ij}$ не зависит от переменных $x_{1j}, \ldots, x_{nj}$.

Пусть $k \in \{1, \ldots, ns\}$, и $(i_1j_1, ..., i_kj_k)$ — набор индексов длины k из множества $\{11, \ldots, n1, \ldots, 1s, \ldots, ns\}$.

Определим множество $C^k_{i_1j_1,\dots,i_kj_k}$ следующим образом:

$C^k_{i_1j_1,\dots,i_kj_k} = \{\mathbf{C_F} \mid (f_{i_1j_1} + c_{i_1j_1}, \dots, f_{i_kj_k} + c_{i_kj_k})$ — сбалансированная функция из $\mathbb{F}_2^{ns}$ в $\mathbb{F}_2^k\}$.

Рассмотрим следующее множество:

$$\mathbf{C} = \bigcap_k \bigcap_{i_1j_1,\dots,i_kj_k} C^k_{i_1j_1,\dots,i_kj_k}.$$

Теорема 11. *Функция* $\mathbf{F} + \mathbf{C_F}$ *взаимно однозначна тогда и только тогда, когда* $\mathbf{C_F} \in \mathbf{C}$.

Доказательство.

$\Leftarrow$ По определению множества $\mathbf{C}$ для любой функции $\mathbf{C_F} \in \mathbf{C}$ функция $\mathbf{F} + \mathbf{C_F}$ обладает тем свойством, что для любого $k \in \{1, \dots, ns\}$ и для любого набора индексов $(i_1j_1, ..., i_kj_k)$ из множества $\{11, \dots, n1, \dots, 1s, \dots, ns\}$, векторная функция $(f_{i_1j_1} + c_{i_1j_1}, ..., f_{i_kj_k} + c_{i_kj_k})$ сбалансирована. Следовательно, из замечания выше следует, что функция $\mathbf{F} + \mathbf{C_F} = (f_{11} + c_{11}, ..., f_{n1} + c_{n1}, ..., f_{1s} + c_{1s}, ..., f_{ns} + c_{ns})$ взаимно однозначна.

$\Rightarrow$ Пусть функция $\mathbf{F} + \mathbf{C_F}$ взаимно однозначна. Тогда для любого $k \in \{1, \dots, ns\}$ и для любого набора индексов $(i_1j_1, ..., i_kj_k)$ из множества $\{11, \dots, n1, \dots, 1s, \dots, ns\}$ векторная функция $(f_{i_1j_1} + c_{i_1j_1}, ..., f_{i_kj_k} + c_{i_kj_k})$ сбалансирована. Следовательно, функция $\mathbf{C_F}$ принадлежит множеству $C^k_{i_1j_1,\dots,i_kj_k}$ по построению. Значит, в силу произвольности k и набора $(i_1j_1, ..., i_kj_k)$, функция $\mathbf{C_F}$ принадлежит и множеству $\mathbf{C} = \bigcap_k \bigcap_{i_1j_1,\dots,i_kj_k} C^k_{i_1j_1,\dots,i_kj_k}$. □

Данная теорема позволяет нам применить следующий метод поиска (см. Метод 4) возможного равномерного разбиения функции $F = (f_1, \dots, f_n)$, где $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$.

Рассмотрим S-блок $F = (xy + yz + xz, x + y + xy + yz, x + z + yz)$, принадлежащий классу $\mathcal{Q}_3^3$, и применим к нему следующую модификацию Метода 4. Положим $k = 4$ и выберем индексы $(11, 12, 13, 21) \in J_k$. Для данных параметров построим множество $C_1 = C^4_{11,12,13,21}$. В результате работы алгоритма мы получили, что множество C_1 пусто. Следовательно, множество C из условия теоремы — пусто, следовательно, не существует равномерного разбиения для данной функции. Мощность перебора для данной модификации составила 2^{35}.

Таким образом, доказано следующее утверждение:

Утверждение 9. *Для S-блоков из класса* $\mathcal{Q}_3^3$ *не существует равномерного разбиения на 3 части.*

Входные данные: Непосредственное разбиение $\mathbf{F} = (f_{11}, \ldots, f_{1s}, ..., f_{n1}, \ldots, f_{ns})$ функции F на s частей $F_i = (f_{1i}, \ldots, f_{ni})$ и множества J_k, содержащие всевозможные упорядоченные наборы индексов $(i_1j_1, \ldots, i_kj_k)$ из $\{11, \ldots, n1, \ldots, 1s, \ldots, ns\}$ для некоторого $1 \leq k \leq ns$.

Выходные данные: Множество $\mathbf{C}$ такое, что для каждой функции $\mathbf{C_F} \in \mathbf{C}$ разбиение $F'_1 = (f_{11} + c_{11}, \ldots, f_{n1} + c_{n1}), \ldots, F'_s = (f_{1s} + c_{1s}, \ldots, f_{ns} + c_{ns})$ является равномерным.

цикл $k = 1$ **до** ns **выполнять**
  до тех пор, пока $J_k \neq \emptyset$ **выполнять**
    Выбрать набор индексов $(i_1j_1, ..., i_kj_k) \in J_k$.
    Присвоить $J_k := J_k \backslash (i_1j_1, ..., i_kj_k)$.
    Построить множество $C^k_{i_1j_1,...,i_kj_k} = \{\mathbf{C_F} \mid (f_{i_1j_1} + c_{i_1j_1}, ..., f_{i_kj_k} + c_{i_kj_k}) -$ является сбалансированной функцией $\}$.
    $\mathbf{C} := \bigcap_k \bigcap_{i_1j_1,...,i_kj_k} C^k_{i_1j_1,...,i_kj_k}$.
    если $\mathbf{C} \neq \emptyset$ **тогда**
      выход;
    конец
  конец
  если $\mathbf{C} = \emptyset$ **тогда**
    выход;
  конец
конец

Метод 4: Метод поиска равномерного разбиения функции F на s частей

В [13] доказано, что, если не существует равномерного разбиения для S-блоков 3×3 из некоторого класса, то для S-блоков 4×4 из соответствующего ему класса также не существует равномерного разбиения. Классу $\mathcal{Q}^3_3$ соответствует класс $\mathcal{Q}^4_{300}$.

Утверждение 10. *Для S-блоков из класса $\mathcal{Q}^4_{300}$ не существует равномерного разбиения на 3 части.*

5.2.2 Представление S-блока в виде композиций S-блоков, обладающих равномерным разбиением

Предложен метод разбиения S-блоков из класса $\mathcal{Q}^3_3$ в виде композиции двух и трех S-блоков из таких классов аффинной эквивалентности, что для них существует равномерное разбиение. Рассмотрим перестановку

$$\begin{pmatrix} \ldots & i_1 & \ldots & i_2 & \ldots & i_{s-1} & \ldots & i_s & \ldots \\ \ldots & i_2 & \ldots & i_3 & \ldots & i_s & \ldots & i_1 & \ldots \end{pmatrix}$$

где все невыписанные символы остаются на месте. Напомним, что такая перестановка называется циклической подстановкой или циклом, и ее можно записать в виде $(i_1, i_2, \ldots, i_{s-1}, i_s)$.

Известно, что всякая перестановка единственным образом представима в виде произведения независимых циклов, а также, что всякая перестановка представима в виде произведения транспозиций.

Две перестановки σ_1 и σ_2 называются *сопряженными*, если существует такая перестановка π, что $\sigma_1 = \pi\sigma_2\pi^{-1}$. Перестановки σ_1 и σ_2 сопряжены тогда и только тогда, когда они обладают одинаковой циклической структурой (у них равное количество циклов одинаковой длины). Рассмотрим исследуемый S-блок из $\mathcal{Q}_3^3$: $S = (xy+yz+xz, x+y+xy+yz, x+z+yz)$. В циклическом представлении он имеет вид $(34)(567)$. Был найден S-блок S' из класса $\mathcal{Q}_1^3$, имеющий такую же циклическую структуру как и S. Его представление в виде произведения циклов $(27)(134)$, следовательно, S и S' сопряжены некоторой перестановкой $\pi : S = \pi S'\pi^{-1}$. Ее можно найти в явном виде: $\pi = (15)(236)(47)$, причем и она, и ее инверсия $\pi^{-1} = (15)(263)(47)$, принадлежат классу $\mathcal{Q}_2^3$, следовательно, S можно реализовать за три шага, на каждом из которых для S-блока существует разбиение на три части, являющееся равномерным.

Функция π имеет вид: $\pi = (x + z + xy, x + y + xy + xz, x + y + z + xz)$. Равномерное разбиение для π следующее (корректирующие слагаемые выделены подчеркиванием):

$\pi_1(v) = (x_2 + z_2 + x_2y_2 + x_2y_3 + x_3y_2 + \underline{y_3} + \underline{z_2} + \underline{z_3}, x_2 + y_2 + y_2x_2 + y_2x_3 + y_3x_2 + z_2x_2 + z_2x_3 + z_3x_2 + \underline{y_3} + \underline{z_3}, x_2 + y_2 + z_2 + z_2x_2 + z_2x_3 + z_3x_2 + \underline{z_2})$,

$\pi_2(v) = (x_3 + z_3 + x_3y_3 + x_1y_3 + x_3y_1 + \underline{y_3} + \underline{z_1} + \underline{z_3}, x_3 + y_3 + y_3x_3 + y_1x_3 + y_3x_1 + z_3x_3 + z_1x_3 + z_3x_1 + \underline{y_3} + \underline{z_3}, x_3 + y_3 + z_3 + z_3x_3 + z_1x_3 + z_3x_1 + \underline{z_1})$,

$\pi_3(v) = (x_1 + z_1 + x_1y_1 + x_2y_1 + x_1y_2 + \underline{z_1} + \underline{z_2}, x_1 + y_1 + y_1x_1 + y_2x_1 + y_1x_2 + z_1x_1 + z_1x_2 + z_2x_1, x_1 + y_1 + z_1 + z_1x_1 + z_2x_1 + z_1x_2 + \underline{z_1} + \underline{z_2})$.

Функция $S' = (y + xz, y + z + zx, x + y + z + zx)$. Равномерное разбиение для S' строится методом непосредственного разбиения, без корректирующих слагаемых:

$S'_1(v) = (y_2 + z_2x_2 + z_2x_3 + z_3x_2, y_2 + z_2 + z_2x_2 + z_2x_3 + z_3x_2, x_2 + y_2 + z_2 + z_2x_2 + z_2x_3 + z_3x_2)$,

$S'_2(v) = (y_3+z_3x_3+z_1x_3+z_3x_1, y_3+z_3+z_3x_3+z_1x_3+z_3x_1, x_3+y_3+z_3+z_1x_3+z_3x_1)$,

$S'_3(v) = (y_1 + z_1x_1 + z_1x_2 + z_2x_1, y_1 + z_1 + z_1x_1 + z_1x_2 + z_2x_1, x_1 + y_1 + z_1 + z_1x_1 + z_1x_2 + z_2x_1)$.

Функция $\pi^{-1} = (x + y + z, x + y + xy + xz, x + z + xz + yz)$. Равномерное разбиение для π^{-1} следующее:

$\pi_1^{-1}(v) = (x_2 + y_2 + z_2, x_2 + y_2 + y_2x_2 + y_2x_3 + y_3x_2 + z_2x_2 + z_2x_3 + z_3x_2 + \underline{y_3} + \underline{z_3}, x_2 + z_2 + z_2x_2 + z_2x_3 + z_3x_2 + y_2z_2 + y_2z_3 + y_3z_2 + \underline{z_2})$,

$\pi_2^{-1}(v) = (x_3 + y_3 + z_3, x_3 + y_3 + y_3x_3 + y_1x_3 + y_3x_1 + z_3x_3 + z_1x_3 + z_3x_1 + \underline{y_3} + \underline{z_3}, x_3 + z_3 + z_3x_3 + z_1x_3 + z_3x_1 + y_3z_3 + y_1z_3 + y_3z_1 + \underline{z_1})$,

$\pi_3^{-1}(v) = (x_1 + y_1 + z_1, x_1 + y_1 + y_1x_1 + y_2x_1 + y_1x_2 + z_1x_1 + z_1x_2 + z_2x_1, x_1, z_1 + z_1x_1 + z_2x_1 + z_1x_2 + y_1z_1 + y_2z_1 + y_1z_2 + \underline{z_1} + \underline{z_2})$.

Также установлено, что перестановка $S'' = \pi S' = (1537)(264)$ принадлежит к классу $\mathcal{Q}_1^3$, а значит, $S = S''\pi^{-1}$ можно реализовать за два шага, для каждого из которых существует равномерное разбиение. Функция $S'' = (y + z + yz + xz, x + y, z)$. Равномерное разбиение для S'' также не требует корректирующих слагаемых:

$S_1''(v) = (y_2 + z_2 + z_2x_2 + z_2x_3 + z_3x_2 + y_2z_2 + y_2z_3 + y_3z_2, x_2 + y_2, z_2)$,

$S_2''(v) = (y_3 + z_3 + z_3x_3 + z_1x_3 + z_3x_1 + y_3z_3 + y_1z_3 + y_3z_1, x_3 + y_3, z_3)$,

$S_3''(v) = (y_1 + z_1 + z_1x_1 + z_1x_2 + z_2x_1 + y_1z_1 + y_2z_1 + y_1z_2, x_1 + y_1, z_1)$.

Поскольку данная конструкция под действием аффинного преобразования остается в рамках тех же классов, то справедливо следующее:

Утверждение 11. *Любой S-блок из класса $\mathcal{Q}_3^3$ можно представить как композицию двух S-блоков — из классов $\mathcal{Q}_1^3$ и $\mathcal{Q}_2^3$, для каждого из которых существует равномерное разбиение на три части.*

Заключение

Приведем список основных результатов данной работы.

1. Предложен метод построения взаимно однозначных APN-функций с помощью 2-в-1 векторных функций, полученных из символьных последовательностей специального вида.

2. Описан метод построения взаимно однозначных APN-функций с помощью векторных функций из специального подкласса, представимых в виде $S = (s_1, \ldots, s_{n-1})$, и недостающих координатных булевых функций s_n. Получена оценка числа таких булевых функций s_n, что взаимно однозначная функция $H = (s_1, \ldots, s_n)$ является APN-функцией. Доказано, что любая APN-перестановка может быть построена данным методом.

3. Доказана верхняя оценка числа координатных симметрических булевых функций у APN-функций и координатных функций, инвариантных относительно циклического сдвига. Получена нижняя оценка числа различных значений APN-функции, получены верхние оценки мощностей прообразов ее значений.

4. Предложена оптимизация поиска равномерного разбиения векторных функций, используемого в методе пороговой реализации. Доказано, что не существует равномерного разбиения на 3 части для одного из классов аффинной эквивалентности S-блоков 3×3. Предложен общий метод построения равномерных разбиений векторных булевых функций путем их декомпозиции.

Литература

1. Глухов М. М. О приближении дискретных функций линейными функциями // Математические вопросы криптографии. 2016. Т. 7, В. 4, С. 29–50.

2. Глухов М. М. О матрицах переходов разностей при использовании некоторых модулярных групп // Математические вопросы криптографии. 2013. Т. 4, В. 4, С. 27–47.

3. Городилова А. А. Характеризация почти совершенно нелинейных функций через подфункции // Дискретная математика. 2015. Т. 27, В. 3, С. 3–16.

4. Тужилин М. Э. Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. Т. 5, В. 3, С. 14–20.

5. Agievich S., Gorodilova A., Kolomeec N., Nikova S., Preneel B., Rijmen V., Shushuev G., Tokareva N., Vitkup V. Problems, solutions and experience of the first international student's Olympiad in cryptography // Прикладная дискретная математика. 2015. Т. 29, В. 3, С. 15–28.

6. Akkar M.-L., Giraud C. An implementation of DES and AES, secure against some attacks // Proceedings of Cryptographic Hardware and Embedded Systems (CHES'01), Lecture Notes in Computer Science. 2001. V. 2162, P. 309-–318.

7. Berger T., Canteaut A., Charpin P., Laigle-Chapuy Y.: On almost perfect nonlinear functions over $\mathbb{F}_{2^n}$ // IEEE Trans. Inform. Theory. 2006. V. 52(9), P. 4160–4170 (2006).

8. Bertoni G.,Daemen J.,Peeters M.,VanAssche G.: Building power analysis resistant implementations of KECCAK // Proceedings of The Second SHA-3 candidate conference. 2010.

9. Beth T., Ding C. On almost perfect nonlinear permutations // Proceedings of EUROCRYPT'93, Lecture Notes in Computer Science. Springer-Verlag, New York. 1993. V. 765. P. 65–76.

10. Bilgin B., Nikova S., Nikov V., Rijmen V., Tokareva N., Vitkup V. Threshold implementations of small S-boxes // Cryptography and Communications. 2015. V. 7. I. 1. P. 3–33.

11. Bilgin B., Daemen J., Nikov V., Nikova S., Rijmen V., Van Assche G.: Efficient and first-order DPA resistant implementations of KECCAK // Proceedings of Smart Card Research and Advanced Applications (CARDIS'13), Lecture Notes in Computer Science. V. 8419, P. 187–199.

12. Bilgin B., Bogdanov A., Knežević M., Mendel F., Wang Q. Fides: Lightweight Authenticated Cipher with Side-Channel Resistance for Constrained Hardware // Proceedings of Cryptographic Hardware and Embedded Systems (CHES'13), Lecture Notes in Computer Science. 2013. V. 8086.

13. Bilgin B., Nikova S., Nikov V., Rijmen V., St'utz G.: Threshold implementations of all 3x3 and 4x4 s-boxes // Proceedings of Cryptographic Hardware and Embedded Systems (CHES'12), Lecture Notes in Computer Science. V. 7428 of Lecture Notes in Computer Science, P. 76–91.

14. Bilgin B., Gierlichs B., Nikova S., Nikov V., Rijmen V.: A more efficient AES threshold implementation // Proceedings of AFRICACRYPT'14, Lecture Notes in Computer Science. 2014. V. 8469, P. 267–284.

15. Biham E., Shamir A.: Differential cryptanalysis of DES-like cryptosystems // Journal of Cryptology. 1991. V. 4(1), P. 3–72.

16. Biryukov A., De Canni'ere C., Braeken A., Preneel B.: A Toolbox for Cryptanalysis: Linear and Affine Equivalence Algorithms // Proceedings of EUROCRYPT'03, Warsaw, Poland, May 4-8, 2003, P. 33–50.

17. Blomer J., Guajardo J., Krummel V.: Provably secure masking of AES //Proceedings SAC'04, Lecture Notes in Computer Science. 2005. P. 69–83.

18. Blondeau C., Canteaut A., Charpin P.: Differential properties of $x \mapsto x^{2^t-1}$ // IEEE Trans. Inf. Theory. 2011. V. 57(12), P. 8127–8137.

19. Blondeau C. and Nyberg K. Perfect nonlinear functions and cryptography // Finite Fields and their Applications. 2015. V. 32, P. 120–147.

20. Braeken A. Cryptographic Properties of Boolean Functions and S-boxes. PhD thesis, Katholieke Universiteit Leuven, 2006.

21. Brinkman M., Leander G. On the classification of APN functions up to dimension five // Proceedings of the International Workshop on Coding and Cryptography 2007 dedicated to the memory of Hans Dobbertin (Versailles, France, 2007). P. 39–48.

22. Browning K. A., Dillon J. F., Kibler R. E., McQuistan M. T. APN Polynomials and Related Codes // J. Combinatorics, Information and System Science, Special Issue in honor of Prof. D.K Ray-Chaudhuri on the occasion of his 75th birthday. 2009. V. 34, No1–4. P. 135–159.

23. Browning K. A., Dillon J. F., McQuistan M. T., Wolfe A. J. An APN Permutation in Dimension Six // Post-proceedings of the 9-th International Conference on Finite Fields and Their Applications Fq'09, Contemporary Math., AMS. 2010. V. 518, P. 33–42.

24. Budaghyan L. Construction and analysis of cryptographic functions. Springer International Publishing. 2014, 168 p.

25. Budaghyan L., Carlet C. CCZ-equivalence of single and multi output Boolean functions // Post-proceedings of the 9-th International Conference on Finite Fields and Their Applications Fq'09, Contemporary Math., AMS. 2010. V. 518, P. 43–54.

26. Budaghyan L., Carlet C., Leander G. Constructing new APN functions from known ones // Finite Fields and Their Applications. 2009. V. 15, I. 2, P. 150–159.

27. Budaghyan L., Carlet C., Pott A. New classes of almost bent and almost perfect nonlinear polynomials // IEEE Trans. Inform. Theory. 2006. V. 52, P. 1141–1152.

28. Budaghyan L, Carlet C, Helleseth T, Li N, Sun B: On Upper Bounds for Algebraic Degrees of APN Functions // IEEE Trans. Information Theory. 2018. V. 64(6), P. 4399–4411.

29. Calderini M., Sala M., Villa I: A note on APN permutations in even dimension // Finite Fields and Their Applications. 2017. V. 46, P. 1–16.

30. Canteaut A., Charpin P., Dobbertin H. Binary m-sequences with three-valued crosscorrelation: a proof of Welch conjecture // IEEE Trans. Inf. Theory. 2000. V. 46. I. 1. P. 4–8.

31. Canteaut A., Duval S., Perrin L.: A generalisation of Dillon's APN permutation with the best known differential and linear properties for all fields of size 2^{4k+2} // IEEE Trans. Information Theory V. 63. I. 11. P. 7575–7591.

32. Carlet C. Boolean Functions for Cryptography and Error Correcting Codes, Ch. 8 of the monograph “Boolean Methods and Models in Mathematics, Computer Science, and Engineering”, Cambridge Univ. Press, 2010. P. 257–397.

33. Carlet C, Partially-bent functions // Proceedings of CRYPTO’92, Advances in Cryptology, Lecture Notes in Computer Science. 1993. P. 280–291.

34. Carlet C. Vectorial Boolean functions for cryptography, Ch. 9 of the monograph “Boolean Methods and Models in Mathematics, Computer Science, and Engineering”, Cambridge Univ. Press, 2010. P. 398–472.

35. Carlet C. Open Questions on Nonlinearity and on APN Functions // Arithmetic of Finite Fields, Lecture Notes in Computer Science. 2015. V. 9061. P 83–107.

36. Carlet C., Charpin P., and Zinoviev V. Codes, bent functions and permutations suitable for DES-like cryptosystems // Designs, Codes and Cryptography. 1998. V. 15. P. 125–156.

37. Charpin P. On almost perfect nonlinear functions over F_2^n // IEEE Trans. Inf. Theory. 2006. V. 52, I. 9, P. 4160–4170.

38. Cusick T. W. and Stănică P. Cryptographic Boolean Functions and Applications. Acad. Press. Elsevier, 2009. 245 p.

39. Daemen J., Rijmen V. The Designn of Rijdael: AES — Advanced Encryption Standard. Springer. 2002. 256 p.

40. Dillon J. F. APN polynomials: an update // Proceedings of the 9th International Conference on Finite Fields and Applications (Dublin, Ireland, July). 2009.

41. Dobbertin H. Almost perfect nonlinear power functions over $GF(2^n)$: the Niho case // Information and Computation. 1999. V. 151, I. 1–2, P. 57–72.

42. Dobbertin H. Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case // IEEE Trans. Inf. Theory. 1999. V. 45, I. 4, P. 1271–1275.

43. Dobbertin H.: One-to-One Highly Nonlinear Power Functions on $GF(2^n)$. // Appl. Algebra Eng. Commun. Comput. 1998. vol.9(2), P. 139–152.

44. Dobbertin H. Almost perfect nonlinear power functions on $GF(2^n)$: a new class for n divisible by 5 // Proceedings of Finite Fields and Applications Fq5. 2000. P. 113–121.

45. Edel Y. On quadratic APN functions and dimensional dual hyperovals // Designs, Codes and Cryptoraphy. 2010. V. 57, I. 1, P. 35–44.

46. Edel Y. Quadratic APN functions as subspaces of alternating bilinear forms // Proceedings of the Contact Forum Coding Theory and Cryptography III, Belgium. 2009. P. 1–24. 2011.

47. Edel Y., Pott A. A new almost perfect nonlinear function which is not quadratic // Advances in Mathematics of Communications. 2009. V. 3. I. 1. P. 59–81.

48. Gold R. Maximal recursive sequences with 3-valued recursive crosscorrelation functions // IEEE Trans. Inform. Theory. 1968. V. 14. P. 154–156.

49. Golic J D., Tymen C. Multiplicative masking and power analysis of AES // Proceedings of Cryptographic Hardware and Embedded Systems (CHES 2002), Lecture Notes in Computer Science. 2003. V. 2523, P. 198–212.

50. Gorodilova A. On the differential equivalence of APN functions // Cryptography and communications. Published online. 2018.

51. Hernando F., McGuire G. Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions // Journal of Algebra. 2011. V. 343. I. 1. P. 78–92.

52. Hollmann H., Xiang Q. A proof of the Welch and Niho conjectures on crosscorrelations of binary m-sequences // Finite Fields and Their Applications. 2001. V. 7. P. 253–286.

53. Hou X.-D. Affinity of permutations of $\mathbb{F}_2^n$ // Discret. Appl. Math. 2006. V. 154. P. 313–325.

54. Ishai Y., Sahai A., Wagner D.: Private circuits: Securing hardware against probing attacks // Proceedings of CRYPTO 2003, Lecture Notes in Computer Science. 2003. V. 2729, P. 463–481.

55. Janwa H., Wilson R. Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes // Proceedings of AAECC-10, Lecture Notes in Computer Science. 1993. V. 673, P. 180–194.

56. Kasami T. The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes // Inform. and Control. 1971. V. 18. P. 369–394.

57. Krasnayová D. Constructions of APN permutations. Master Thesis. Charles University, Prague. 2016. 41 p.

58. Lidl R., Niederreiter H.: Finite Fields. Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley, Reading, Massachussetts. 1983. 772 p.

59. Lisoněk P. APN permutations and double simplex codes // Proceedings of Mathematics of Communications: Sequences, Codes and Designs, BIRS, 25–30 January 2015.

60. Meier W., Staffelbach O. Nonlinearity criteria for cryptographic functions // Proceedings of EUROCRYPT'89, Lecture Notes in Computer Science. V. 434. Springer. 1989. P. 549–562.

61. Moradi A., Poschmann A., Ling S., Paar C., Wang H.: Pushing the limits: A very compact and a threshold implementation of AES // Proceedings of EUROCRYPT'11, Lecture Notes in Computer Science. 2011. V. 6632, P. 69–88.

62. Nikova S., Rechberger C., Rijmen V.: Threshold implementations against side-channel attacks and glitches // Information and Communications Security, Lecture Notes in Computer Science. 2006. V. 4307, P. 529–545.

63. Nikova S., Rijmen V., Schläffer M.: Secure hardware implementation of nonlinear functions in the presence of glitches // Proceedings of Information Security and Cryptology (ICISC'08), Lecture Notes in Computer Science. 2009. V. 5461, P. 218–234.

64. Nikova S., Rijmen V., Schläffer M.: Secure hardware implementation of nonlinear functions in the presence of glitches // J. Cryptol. 2011. V. 24, P. 292–321.

65. Nikova S., Nikov V., Rijmen V. Decomposition of Permutations in a Finite Field // Cryptogr. Commun. 2018. published online.

66. Nyberg K. Perfect nonlinear S-boxes // Proceedings of EUROCRYPT'91, Lecture Notes in Computer Science. 1991. V. 547. P. 378–386.

67. Nyberg K. Differentially uniform mappings for cryptography // EUROCRYPT"93. LNCS. 1994. V. 765. P. 55–64.

68. Nyberg K.: S-boxes and Round Functions with Controllable Linearity and Differential Uniformity // Proceedings of FSE'94, Lecture Notes in Computer Science. 1994. V. 765, P. 111–130.

69. Nyberg K., Knudsen L. R. Provable security against differential cryptanalysis // Proceedings of CRYPTO'92, Lecture Notes in Computer Science. 1992. V. 740, P. 566–574.

70. Oswald E., Mangard S., Pramstaller N., Rijmen V.: A side-channel analysis resistant description of the AES S-box // Proceedings of Fast Software Encryption (FSE'05), Lecture Notes in Computer Science. 2005. V. 3557, P. 413–423.

71. Rivain M., Prouff E.: Provably secure higher-order masking of AES // Proceedings of Cryptographic Hardware and Embedded Systems (CHES'10), Lecture Notes in Computer Science. 2010. V. 6225, P. 413–427.

72. Pasalic E., Charpin P.: Some results concerning cryptographically significant mappings over $GF(2^n)$ // Designs, Codes and Cryptography. 2010. V. 57, I. 3, P. 257–269.

73. Perrin L., Udovenko A., Biryukov A. Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem // CRYPTO'16, Part II, Lecture Notes in Computer Science. 2016. V. 9815, P. 93–122.

74. Pieprzyk J., Qu C. X. Fast hashing and rotation-symmetric functions. // Journal of Universal Computer Science. 1999. V. 5. Issue 1. P. 20–31.

75. Popp T., Mangard S.: Masked dual-rail pre-charge logic: DPA-resistance without routing constraints // Proceedings of Cryptographic Hardware and Embedded Systems (CHES'05), Lecture Notes in Computer Science. 2005. V. 3659, P. 172–186.

76. Poschmann A., Moradi A., Khoo K., Lim C.-W., Wang H., Ling S.: Side-channel resistant crypto for less than 2,300 GE // J. Cryptol. 2011. V. 24, I. 2, P. 322–345.

77. Pott A. Almost perfect and planar functions // Designs, Codes and Cryptography. 2016. V. 78. P. 141–195.

78. Tiri K. and Verbauwhede I. A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation // Proceedings of the Conference on Design, Automation and Test in Europe (DATE '04), IEEE Computer Society. 2004. P. 10246.

79. Zheng Y. and Zhang X. M. Plateaued functions // Proceedings of ICICS'99, Lecture Notes in Computer Science. 1999. V. 1726, P. 284–300.

Публикации автора по теме диссертации

Статьи из списка ВАК

78. Bilgin B., Nikova, S., Nikov, V., Rijmen V., Tokareva N., Vitkup V. Threshold implementations of small S-boxes // Cryptography and Communications. 2015. V. 7. N. 1. P. 3–33.

79. Виткуп В. А. О симметрических свойствах APN-функций // Дискретный анализ и исследование операций. 2016. Т. 23. № 2. С. 5–21. (Перевод: Vitkup V. A. On symmetric properties of APN functions // Journal of Applied and Industrial Mathematics. 2016. V. 2. I. 2. P. 5–21.)

80. Идрисова В. А. О построении APN-перестановок с помощью подфункций // Прикладная дискретная математика. 2018. Т. 41. № 2. С. 17–27.

81. Idrisova V. On an algorithm generating 2-to-1 APN functions and its applications to “the big APN problem” // Cryptography and Communications. 2018, опубликована онлайн 11 мая, DOI: 10.1007/s12095-018-0310-9/.

Тезисы конференций

82. Виткуп В. А. О представлении S-блоков при реализации в блочных шифрах // Прикладная дискретная математика. Приложение. 2013. № 6. С. 30–32.

83. Виткуп В. А. О некоторых открытых вопросах в области APN-функций // Прикладная дискретная математика. Приложение. 2014. № 7. С. 11–13.

84. Vitkup V. A. On Threshold Implementations of vectorial Boolean functions in cryptographic primitives // Proc. of «Mal’tsev meeting» (Novosibirsk, November 11–15, 2013). C. 46.

85. Виткуп В. А. О числе симметрических координатных функций APN-функции // Прикладная дискретная математика. Приложение. 2015. № 8. С. 23–25.

86. Виткуп В. А. О специальном подклассе векторных булевых функций и проблеме существования APN-перестановок // Прикладная дискретная математика. Приложение. 2016. № 9. С. 19–21.

87. Идрисова В. А. О построении APN-функций специального вида и их связи с взаимно однозначными APN-функциями // Прикладная дискретная математика. Приложение. 2017. № 10. С. 36–38.

88. Idrisova V. On APN functions EA-equivalent to permutations // Proceedings of the 2nd workshop Boolean Functions and their Applications (BFA), Os, Norway, July 3-8, 2017. P. 24.

89. Идрисова В. А. Векторные 2-в-1 функции как подфункции взаимно однозначных APN-функций // Прикладная дискретная математика. Приложение. 2018. № 11. С. 39–41.

90. Idrisova V. 2-to-1 functions as subfunctions of APN permutations // Proceedings of the 3rd workshop Boolean Functions and their Applications (BFA), Loen, Norway, June 17-22, 2018. P. 4.