На правах рукописи

Идрисова Валерия Александровна

О построении почти совершенно нелинейных векторных функций и их симметрических свойствах

Специальность 01.01.09 — Дискретная математика и математическая кибернетика

Автореферат

диссертации на соискание учёной степени

кандидата физико-математических наук

Новосибирск — 2018

Работа выполнена в Федеральном государственном бюджетном учреждении науки Институте математики им. С. Л. Соболева Сибирского отделения Российской академии наук (ИМ СО РАН)

Научный руководитель: **Токарева Наталья Николаевна**,
кандидат физико-математических наук, с.н.с.

Официальные оппоненты: **Фомичев Владимир Михайлович**,
доктор физико-математических наук, профессор,
Финансовый университет при Правительстве Российской Федерации.

Панкратова Ирина Анатольевна,
кандидат физико-математических наук, доцент,
Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский Томский государственный университет».

Ведущая организация: Институт проблем информационной безопасности при Федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Московском государственном университете имени М. В. Ломоносова».

Защита состоится 23 января 2019 г. в 17 час. 00 мин. на заседании диссертационного совета Д 003.015.01 при Федеральном государственном бюджетном учреждении науки Институте математики им. С. Л. Соболева Сибирского отделения Российской академии наук по адресу: 630090, г. Новосибирск, пр. Академика Коптюга, 4.

С диссертацией можно ознакомиться в библиотеке Федерального государственного бюджетного учреждения науки Института математики им. С. Л. Соболева Сибирского отделения Российской академии наук и на сайте math.nsc.ru.

Автореферат разослан «__» _____ 2018 г.

Ученый секретарь
диссертационного совета
Д 003.015.01, д.ф.-м.н. Ю. В. Шамардин

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. 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 и обозначения.

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. 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. *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 $\mathbb{F}_2^n$.

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

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

где $a_{i_1,\ldots,i_k},\ a_0 \in \mathbb{F}_2^m$. *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 $D_a F(x) = F(x+a) + F(x)$, где a — ненулевой

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

Название	Значение d	Условия
Голда	2^t+1	$(t,n)=1$
Касами	$2^{2t}-2^t+1$	$(t,n)=1$
Уолша	2^t+3	$n=2t+1$
Нихо	$2^t+2^{\frac{t}{2}}-1$, t чётное $2^t+2^{\frac{3t+1}{2}}-1$, t нечётное	$n=2t+1$
Инверсия	$2^{2t}-1$	$n=2t+1$
Доббертина	$2^{4t}+2^{3t}+2^{2t}+2^t-1$	$n=5t$

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

[1] Carlet C., Charpin P., and Zinoviev V. Codes, bent functions and permutations suitable for DES-like cryptosystems // Des. Codes Cryptogr. — 1998. — V. 15. — P. 125–156.

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:

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

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 K. Nyberg[2] в 1993 году. Если F является APN-функцией, то любая EA-эквивалентная/CCZ-эквивалентная функция также является APN-функцией.

В разное время были получены алгебраические конструкции APN-функций: R. Gold (1968), T. Kasami (1971), H. Dobbertin (1999, 2000), T. Beth и C. Ding (1993), L. Budaghyan, C. Carlet, G. Leander (2008, 2009, 2013), C. Bracken, E. Byrne, N. Markin, G. McGuire (2008, 2011), в частности, наиболее известные представители класса APN-функций — мономиальные функции, то есть функции вида $F(x) = x^d$ (см. Таблицу 1) над конечным полем $GF(2^n)$. Известно[3], 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

[2] Nyberg K. Differentially uniform mappings for cryptography // Eurocrypt'93. LNCS. — 1993. — V. 765. — P. 55–64.

[3] Глухов М. М. О приближении дискретных функций линейными функциями // Математические вопросы криптографии. — 2006. — Т. 7, № 4. — С. 29–50.

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 2006 году[4] 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 году в работе J. F Dillon и др.[5] был найден первый пример APN-перестановки от 6 переменных — данная функция получила название *APN-функции Диллона*. Через несколько лет было рассмотрено[6] [7] бесконечное семейство векторных функций с параметром $\Delta_F \leqslant 4$ 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 взаимно однозначные APN-функции 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

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

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

[6] 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 Transactions on Information Theory — 2016. — V. 63. — P. 7575–7591.

[7] Perrin L., Udovenko A., Biryukov A. Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem // In Matthew Robshaw and Jonathan Katz, editors, Advances in Cryptology — CRYPTO 2016, Part II, Lecture Notes in Computer Science. — 2016. — V. 9815. — P. 93–122.

вносят изменения в исследуемые криптоаналитиком параметры, например, добавляют временные задержки в расписание вычислений или вставляют в алгоритм дополнительные операции. Также известны[8] 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, так и в дизайне аппаратного устройства. Одним из самых перспективных способов маскирования блочного шифра является метод пороговой реализации[9], который представляет собой специальное равномерное разбиение S-блоков. Данный метод обладает рядом достоинств: он не привязан к конкретной аппаратной реализации, защищен от случайных сбоев, а также позволяет сохранять компактность аппаратного устройства.

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.

[8] 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 Conference and Exhibition. — 2004. — P. 10246.

[9] Nikova S., Rechberger, C., Rijmen V. Threshold implementations against side-channel attacks and glitches. // In: Ning, P., Qing, S., Li, N. (eds.) Information and Communications Security, Lecture Notes in Computer Science. — 2006. — V. 4307. — P. 529–545.

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.

Методика исследований. В диссертации используются комбинаторные методы и методы дискретного анализа, а также аппарат алгебры.

Научная новизна и значимость. Вопрос существования взаимно однозначных APN-функций от четного числа переменных является центральным[10] открытым вопросом в области векторных булевых функций. Напомним, что уже при $n = 6$ про класс APN-функций практически ничего неизвестно — классификация APN-функция получена[11] 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 C. Carlet, P. Charpin и В. Зиновьева[12] и явным образом сформулирована через год в работе H. Dobbertin[13]. Долгое время считалось, что не существует взаимно однозначных APN-функций для четных n. Данная гипотеза была вычислительно доказана для $n = 4$, однако, первое теоретическое доказательство того, что не существует APN-перестановок от 4 переменных, появилось лишь в 2017 году[14]. Заметим, что ввиду Теоремы 2 любая $(n-1)$-подфункция APN-перестановки является 2-в-1 дифференциально 4-равномерной функцией, которая принимает значения исключительно из множества $\{0, \ldots, 2^{n-1} - 1\}$. В данной работе получено, что при $n = 4$ таких

[10] Carlet C. Open Questions on Nonlinearity and on APN Functions // Arithmetic of Finite Fields, LNCS. — 2015. — V. 906. — P. 83–107.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

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

Первый пример APN-перестановки от 6 переменных — APN-функция Диллона, был найден лишь в 2009 году. 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[15]. 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[16] [17] через несколько лет и содержащее APN-функцию Диллона, было построено уже с помощью некоторой конструкции над конечным полем. Кроме того, были найдены[18] [19] 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 построения взаимно однозначных APN-функций для любого n — как четного, так и нечетного. Первый метод строит APN-перестановки через сумму 2-в-1 APN-функций и аффинных векторных функций, а второй метод 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

[15] 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. — 2017. — V. 8086. — P. 142–158.

[16] Perrin L., Udovenko A., Biryukov A. Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem // In Matthew Robshaw and Jonathan Katz, editors, Advances in Cryptology - CRYPTO 2016, Part II, Lecture Notes in Computer Science. — 2016. — V. 9815. — P. 93–122.

[17] 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 Transactions on Information Theory — 2016. — V. 63. — P. 7575–7591.

[18] Krasnayová D. Constructions of APN permutations. Master Thesis. Charles University, Prague. — 2016 — 41 p.

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

APN-функция может быть построена с помощью второго метода. Кроме того, в данной работе показано, что APN-функция Диллона может быть построена с помощью первого метода, как и все существующие APN-перестановки от 5 переменных.

Помимо того, что при $n = 4$ не существует 2-в-1 дифференциально 4-равномерных функций, которые принимают значения из множества $\{0, \ldots, 2^{n-1} - 1\}$, 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 однозначных APN-функций может быть сведена к существованию 2-в-1 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 также предложен специальный алгоритм.

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 2006 году 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[20], пока в данной работе не удалось получить теоретический результат, 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, 4 из которых изданы в журналах, рекомендованных ВАК, 9 — в тезисах и трудах конференций.

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.

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

[20] Bilgin B., Nikova S., Nikov V., Rijmen V., Stütz G. Threshold implementations of all 3x3 and 4x4 s-boxes // Proceedings of Cryptographic Hardware and Embedded Systems (CHES'12), Lecture Notes in Computer Science. — 2012. — P. 76–91.

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.

Объём и структура работы. Диссертация состоит из введения, пяти глав, заключения и списка литературы. Объём диссертации 85 страниц. Список литературы содержит 90 наименований.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность исследований, проводимых в рамках данной диссертационной работы, приводится обзор научной литературы по изучаемой проблеме, формулируется цель работы.

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.

Результаты главы 2 опубликованы в [4], [9, 10, 11].

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 главы. 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 $n(S) \geqslant 2^n$.

Результаты главы 3 опубликованы в [3], [4], [12, 13].

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 существо-

вания 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*[21] или *RotS-функция*), 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.

Результаты главы 4 опубликованы в [2], [8].

В **пятой главе** рассматривается метод разбиения S-блоков для защиты от атак по сторонним каналам. Многие криптографические алгоритмы

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

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 S. Nikova и др.[22] описан один из таких методов — пороговая реализация S-блоков.

Рассмотрим 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, $\mathcal{A}_1^3$, $\mathcal{Q}_1^3$, $\mathcal{Q}_2^3$, $\mathcal{Q}_3^3$ [23].

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)

[22] Nikova S., Rechberger, C., Rijmen V. Threshold implementations against side-channel attacks and glitches. // In: Ning, P., Qing, S., Li, N. (eds.) Information and Communications Security, Lecture Notes in Computer Science. — 2006. — V. 4307. — P. 529–545.

[23] 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.

Для всех классов, кроме $\mathcal{Q}_3^3$, ранее[24] было найдено равномерное разбиение. Однако большой перебор не позволял найти для класса $\mathcal{Q}_3^3$ соответствующее разбиение или доказать, что его не существует.

В данной главе предложен способ 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.

Результаты главы 5 опубликованы в [1], [5, 7].

В **заключении** приведены основные результаты работы.

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.

[24] Bilgin B., Nikova S., Nikov V., Rijmen V., Stütz G. Threshold implementations of all 3x3 and 4x4 s-boxes // Proceedings of Cryptographic Hardware and Embedded Systems (CHES'12), Lecture Notes in Computer Science. — 2012. — P. 76–91.

Публикации автора по теме диссертации

Статьи в рецензируемых журналах из списка ВАК

1. 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.

2. 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.)

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

4. 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 и труды конференций

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

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

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

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

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

10. 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.

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

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

13. 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). — 2018. — P. 4.

Идрисова Валерия Александровна

О построении почти совершенно нелинейных векторных функций и их симметрических свойствах

Автореферат диссертации
на соискание ученой степени
кандидата физико-математических наук

Подписано в печать 12.11.2018. Формат 60×84 1/16.
Усл. печ. л. 1,0. Уч.-изд. л. 1,0. Тираж 100 экз. Заказ № .

Отпечатано в ООО "Омега Принт"
пр. Ак. Лаврентьева, 6, Новосибирск 630090