

элемента « ψ », который вычисляет значение функции ψ от элемента кольца, дешифратора (декодера), который записывает значение, полученное сверху, по адресу, полученному справа. Столбец значений функции $f_{u,v,\psi}$ полностью заполняется за $2^m - 1$ тактов работы регистра сдвига.

ЛИТЕРАТУРА

1. Былков Д. Н. Об одном классе булевых функций, построенных с использованием старших разрядных последовательностей линейных рекуррент // Прикладная дискретная математика. Приложение. 2014. № 7. С. 59–60.
2. Былков Д. Н., Камловский О. В. Параметры булевых функций, построенных с использованием старших координатных последовательностей линейных рекуррент // Математические вопросы криптографии. 2012. Т. 3. № 4. С. 25–53.
3. Нечаев А. А. Цикловые типы линейных подстановок над конечными коммутативными кольцами // Матем. сборник. 1993. Т. 184. № 3. С. 21–56.
4. Нечаев А. А. Код Кердока в циклической форме // Дискретная математика. 1989. Т. 1. № 4. С. 123–139.
5. Погорелов Б. А., Сачков В. Н. Словарь криптографических терминов. М.: МЦНМО, 2006.
6. Кузьмин А. С., Нечаев А. А. Линейные рекуррентные последовательности над кольцами Галуа // Алгебра и логика. 1995. Т. 34. № 2. С. 169–189.
7. Камловский О. В. Частотные характеристики разрядных последовательностей линейных рекуррент над кольцами Галуа // Изв. РАН. Сер. матем. 2013. Т. 77. № 6. С. 71–96.

УДК 519.7

DOI 10.17223/2226308X/11/11

ВЕКТОРНЫЕ 2-В-1 ФУНКЦИИ КАК ПОДФУНКЦИИ ВЗАИМНО ОДНОЗНАЧНЫХ APN-ФУНКЦИЙ¹

В. А. Идрисова

Работа посвящена проблеме существования взаимно однозначных APN-функций от чётного числа переменных. Рассматриваются свойства подфункций взаимно однозначных APN-функций. Доказано, что любая $(n - 1)$ -подфункция произвольной взаимно однозначной APN-функции может быть получена при помощи специальных символьных последовательностей. Данные результаты позволяют предложить новый алгоритм построения взаимно однозначных APN-функций из 2-в-1 функций и соответствующих координатных булевых функций. Получена нижняя оценка на число таких булевых функций.

Ключевые слова: векторная булева функция, APN-функция, взаимно однозначная функция, 2-в-1 функция, перестановка.

Векторной булевой функцией F называется произвольное отображение $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$. Рассмотрим векторную булеву функцию F из \mathbb{F}_2^n в \mathbb{F}_2^m . Для векторов $a, b \in \mathbb{F}_2^m$, где $a \neq \mathbf{0}$, определим величину

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

Обозначим за Δ_F следующий параметр:

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

¹Работа поддержана грантом РФФИ, проект № 17-41-543364.

Тогда F называется *дифференциально Δ_F -равномерной* функцией. Чем меньше параметр Δ_F , тем более устойчив к дифференциальному криптоанализу блочный шифр, содержащий функцию F в качестве S -блока. Для векторных функций из \mathbb{F}_2^n в \mathbb{F}_2^n минимально возможное значение Δ_F равно 2. В этом случае функция F называется *почти совершенно нелинейной* функцией, или *APN-функцией*. Данные понятия введены К. Ньюбергом в [1], однако известно [2], что APN-функции также изучались В. А. Башевым и Б. А. Егоровым в СССР в 60-х годах. Подробнее об APN-функциях можно прочесть в [3–5].

Одна из самых интересных проблем в данной области связана со взаимно однозначными APN-функциями [6]. Долгое время имела место гипотеза, что не существует взаимно однозначных APN-функций от чётного числа переменных. Однако в 2009 г. авторы работы [7] нашли первый и единственный (с точностью до эквивалентности) на данный момент пример взаимно однозначной APN-функции над \mathbb{F}_2^6 . Для больших размерностей вопрос существования по-прежнему открыт.

Векторная функция $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ называется *2-в-1 функцией*, если её множество значений состоит из 2^{n-1} элементов и каждое значение она принимает ровно на двух аргументах.

Рассмотрим произвольную векторную функцию $F = (f_1, \dots, f_n)$ из \mathbb{F}_2^n в \mathbb{F}_2^n . Будем называть векторную булеву функцию F'_j из \mathbb{F}_2^n в \mathbb{F}_2^{n-1} ($n-1$)-*подфункцией* функции F , если $F'_j = (f_1, \dots, f_{j-1}, f_{j+1}, \dots, f_n)$ для некоторого $j \in \{1, \dots, n\}$. Напомним, что множеству \mathbb{F}_2^n можно сопоставить во взаимно однозначное соответствие целочисленное множество $\{0, \dots, 2^n - 1\}$, где каждое число является десятичным представлением вектора из \mathbb{F}_2^n . Тогда произвольную $(n-1)$ -подфункцию F'_j из \mathbb{F}_2^n в \mathbb{F}_2^{n-1} можно рассматривать как векторную функцию из \mathbb{F}_2^n в \mathbb{F}_2^n , принимающую значения из множества $\{0, \dots, 2^{n-1} - 1\}$.

Рассмотрим произвольную 2-в-1 функцию, принимающую значения из $\{0, \dots, 2^{n-1} - 1\}$, тогда вектор её значений может быть представлен в виде некоторой перестановки упорядоченного вектора $(0, 0, 1, 1, \dots, 2^{n-1} - 1, 2^{n-1} - 1)$. Будем обозначать множество таких 2-в-1 функций от n переменных через \mathcal{T}_n . Можно заметить, что тогда любая $(n-1)$ -подфункция взаимно однозначной векторной функции принадлежит \mathcal{T}_n . Имеет место следующее утверждение [8].

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

В [8, 9] рассматривается алгоритм построения 2-в-1 APN-функций при помощи специальных так называемых *допустимых* символьных последовательностей. В [8] доказана следующая

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

Таким образом, любая взаимно однозначная APN-функция может быть получена из некоторой 2-в-1 дифференциально 4-равномерной функции, построенной при помощи допустимой последовательности. Данное наблюдение позволяет предложить следующий алгоритм для поиска новых взаимно однозначных APN-функций.

С помощью аппарата допустимых последовательностей строим 2-в-1 векторную функцию S , принадлежащую \mathcal{T}_n (подробнее о данном построении см. в [8]) и про-

веряем её на дифференциальную равномерность. Если S дифференциально 4-равномерная, то она может являться $(n - 1)$ -подфункцией некоторой взаимно однозначной APN-функции. Необходимо проверить, существует ли сбалансированная булева функция f , такая, что взаимно однозначная функция $H = S \cup f$ является APN-функцией. Заметим, что требуется проверить $2^{2^{n-1}}$ булевых функций, поскольку на каждую пару одинаковых значений 2-в-1 функции S приходится пара $\{0, 1\}$ из значений булевой функции f .

Обозначим через $nf(S)$ число булевых функций f , таких, что $H = S \cup f$ является взаимно однозначной APN-функцией. Получена следующая нижняя оценка для данной величины:

Теорема 2. Пусть S — векторная функция из \mathcal{T}_n , построенная с помощью допустимой последовательности. Тогда если $nf(S) \neq 0$, то $nf(S) \geq 2^n$.

С помощью компьютерных вычислений проверено, что данная оценка является точной при $n = 3, 5$, а также при $n = 6$ для всех $(n - 1)$ -подфункций APN-функции Диллона.

ЛИТЕРАТУРА

1. Nyberg K. Differently uniform mappings for cryptography // Eurocrypt 1993. LNCS. 1994. V. 765. P. 55–64.
2. Глухов М. М. О приближении дискретных функций линейными функциями // Математические вопросы криптографии. 2016. Т. 7. № 4. С. 29–50.
3. Blondeau C. and Nyberg K. Perfect nonlinear functions and cryptography // Fields and Their Appl. 2015. V. 32. P. 120–147.
4. Тузиллин М. Э. Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. № 3(5). С. 14–20.
5. Pott A. Almost perfect and planar functions // Des. Codes Cryptography. 2016. No. 78(1). P. 141–195.
6. Carlet C. Open questions on nonlinearity and on APN functions // LNCS. 2015. V. 9061. P. 83–107.
7. McQuistan M. T., Wolfe A. J., Browning K. A., and Dillon J. F. An apn permutation in dimension six // Amer. Math. Soc. 2010. No. 518. P. 33–42.
8. Idrisova V. A. On an algorithm generating 2-to-1 APN functions and its applications to “the big APN problem” // Cryptography and Communications. 2018. Published online.
9. 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.

УДК 519.7

DOI 10.17223/2226308X/11/12

О НЕКОТОРЫХ СВОЙСТВАХ КОНСТРУКЦИИ БЕНТ-ФУНКЦИЙ С ПОМОЩЬЮ ПОДПРОСТРАНСТВ ПРОИЗВОЛЬНОЙ РАЗМЕРНОСТИ¹

Н. А. Коломеец

Рассматриваются свойства конструкции $f \oplus \text{Ind}_L$, где f — бент-функция от $2k$ переменных, а L — аффинное подпространство, при определённых условиях порожд-

¹Работа поддержана грантом РФФИ, проект № 17-41-543364.