

10. Potapov V. N. A lower bound on the number of boolean functions with median correlation immunity // 16th Int. Symp. "Problems of redundancy in information and control systems", Moscow, Russia, 2019. P. 45–46.
11. Панков К. Н. Уточнённые асимптотические оценки для числа (n, m, k) -устойчивых двоичных отображений // Прикладная дискретная математика. Приложение. 2017. № 10. С. 46–49.
12. Панков К. Н. Уточнённые асимптотические оценки для числа корреляционно-иммунных двоичных функций и отображений // Прикладная дискретная математика. Приложение. 2018. № 11. С. 49–52.
13. Панков К. Н. Рекуррентные формулы для числа k -эластичных и корреляционно-иммунных двоичных отображений // Прикладная дискретная математика. Приложение. 2019. № 12. С. 62–66.
14. Carlet C. Vectorial Boolean functions for cryptography // Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Encyclopedia of Mathematics and its Applications. V. 134. N.Y.: Cambridge University Press, 2010. P. 398–472.
15. Панков К. Н. Асимптотические оценки для чисел двоичных отображений с заданными криптографическими свойствами // Математические вопросы криптографии. 2014. № 4. С. 73–97.
16. Pankov K. N. Improved asymptotic estimates for the numbers of correlation-immune and k -resilient vectorial Boolean functions // Discr. Math. Appl. 2019. No. 3. P. 195–213.
17. Сачков В. Н. Курс комбинаторного анализа. Ижевск: НИЦ «Регулярная и хаотическая динамика», 2013. 336 с.
18. Панков К. Н. Улучшенные асимптотические оценки для числа корреляционно-иммунных и k -эластичных двоичных вектор-функций // Дискретная математика. 2018. № 2. С. 73–98.

УДК 519.719.2

DOI 10.17223/2226308X/14/9

О СПОСОБЕ ПОСТРОЕНИЯ ДИФФЕРЕНЦИАЛЬНО 2 δ -РАВНОМЕРНЫХ ПОДСТАНОВОК НА $\mathbb{F}_{2^{2m}}$

Д. Б. Фомин

Рассмотрены способы построения дифференциально 2 δ -равномерных подстановок на $\mathbb{F}_{2^{2m}}$ для случая $m \geq 3$. Предложенный подход излагается с использованием так называемого TU -представления функций и обобщает известный способ построения дифференциально 4-равномерных подстановок поля $\mathbb{F}_{2^{2m}}$ с применением подстановки обращения ненулевых элементов поля.

Ключевые слова: *S-Box, подстановка, дифференциальная равномерность, TU-представление.*

Исследование способов построение нелинейных биективных преобразований с заданными криптографическими характеристиками является актуальной и сложной задачей. Одним из известных подходов, позволяющих строить нелинейные преобразования с достаточно высокими криптографическими характеристиками и допускающие эффективную программную и аппаратную реализацию, является использование подстановок, имеющих декомпозицию.

Пусть $\mathbb{F}_2 = \{0, 1\}$ — поле из двух элементов с операциями сложения «+» и умножения «·»; $(\mathbb{F}_2^n, +) = \{(a_0, a_1, \dots, a_{n-1}) : a_i \in \mathbb{F}_2, i = 0, \dots, n-1\}$ — арифметическое векторное пространство размерности n . Задав специальным образом операцию умножения на множестве \mathbb{F}_2^n , можно определить поле \mathbb{F}_{2^n} , состоящее из 2^n элементов. Везде

далее считаем, что фиксирована биекция между \mathbb{F}_2^n и \mathbb{F}_{2^n} . Произвольную функцию $F: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ будем называть (n, m) -функцией. Тогда $(n, 1)$ -функция есть булева функция, биективная (n, n) -функция — подстановка.

Определение 1 [1]. Пусть F — (n, m) -функция, $1 \leq t \leq \min(n, m)$, $x_1, y_1 \in \mathbb{F}_2^t$, $x_2 \in \mathbb{F}_2^{n-t}$, $y_2 \in \mathbb{F}_2^{m-t}$, $x = x_1 \| x_2 \in \mathbb{F}_2^n$, $y = y_1 \| y_2 \in \mathbb{F}_2^m$. Тогда если существуют такие функции $T: \mathbb{F}_2^t \times \mathbb{F}_2^{n-t} \rightarrow \mathbb{F}_2^t$, $U: \mathbb{F}_2^{n-t} \times \mathbb{F}_2^t \rightarrow \mathbb{F}_2^{m-t}$, что при фиксации x_2 произвольным значением $T(x_1, x_2)$ есть биекция по переменной x_1 и функция F представима в виде

$$F(x) = F(x_1 \| x_2) = T(x_1, x_2) \| U(x_2, T(x_1, x_2)), \quad (1)$$

то такое представление функции F в виде (1) будем называть TU -представлением.

Замечание 1. Известно [2], что в случае $m = n$ функция F является подстановкой, если функция $U(x_2, x_1)$ является подстановкой по x_2 при фиксации x_1 .

Определение 2. Для $F: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ и произвольных $a \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$, $b \in \mathbb{F}_2^m$ положим

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

Будем говорить, что F является дифференциальной δ_F -равномерной функцией, если

$$\delta_F = \max_{\substack{a \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}, \\ b \in \mathbb{F}_2^m}} \delta_F^{a,b},$$

значение δ_F будем называть показателем дифференциальной равномерности функции F .

Использование нелинейных преобразований с меньшим показателем дифференциальной δ -равномерности при синтезе криптографических примитивов позволяет гарантировать стойкость последнего к разностному методу криптографического анализа.

Известно достаточно много примеров подстановок, обладающих высокими криптографическими характеристиками и имеющих TU -представление:

- подстановка, *CCZ*-эквивалентная подстановке Диллона, — единственная известная в настоящий момент 2-равномерная подстановка на \mathbb{F}_{2^m} [3];
- подстановка, линейно эквивалентная подстановке алгоритмов ГОСТ Р 34.11-2012 и «Кузнецик» (ГОСТ Р 34.12-2018) [2];
- подстановки из работ [4–7].

Для $a \in \mathbb{F}_2^{n-t}$ обозначим:

- $\delta_{T,a}$ — показатель дифференциальной δ -равномерности подстановки, которую задаёт функция $T(x_1, x_2)$ при фиксации $x_2 = a$;
- $\Delta_{T,a}^{\alpha_1, \alpha_2, \beta_1}$ — количество решений уравнения

$$T(x_1, a) + T(x_1 + \alpha_1, a + \alpha_2) = \beta_1, \quad \alpha_1, \beta_1 \in \mathbb{F}_2^{n-t}, \alpha_2 \in \mathbb{F}_2^t \setminus \{\mathbf{0}\}.$$

Получен следующий критерий дифференциальной δ -равномерности функции F , имеющей TU -представление.

Теорема 1. Пусть у функции F имеется TU -представление (1). Тогда показатель дифференциальной δ -равномерности функции F меньше либо равен значению

$$2^t \cdot \max_{a \in \mathbb{F}_2^t} \left\{ \delta_{T,a}, \max_{\substack{\alpha_1, \beta_1 \in \mathbb{F}_2^{n-t}, \\ \alpha_2 \in \mathbb{F}_2^t \setminus \{\mathbf{0}\}}} \Delta_{T,a}^{\alpha_1, \alpha_2, \beta_1} \right\}.$$

Доказательство теоремы следует из того факта, что при каждой из 2^t фиксаций x_2 значением a_2 уравнения вида

$$T(x_1, a_2) + T(x_1 + \alpha_1, a_2 + \alpha_2) = \beta_1$$

являются следствием уравнений

$$F(x_1, a_2) + F(x_1 + \alpha_1, a_2 + \alpha_2) = \beta_1 \| \beta_2.$$

Теорема 1 позволяет строить дифференциальную 2δ -равномерные преобразования, а замечание 1 гарантирует биективность этого преобразования.

Следствие 1. Пусть в условиях теоремы 1 $t = 1$ и $\delta_{T,a} \leq \delta$ для всех $a \in \mathbb{F}_2$. Тогда функция F , имеющая TU -представление (1), не более чем дифференциальная 2δ -равномерна тогда и только тогда, когда $\max_{\alpha_1, \beta_1 \in \mathbb{F}_2^{n-1}} \Delta_{T,0}^{\alpha_1, \beta_1} \leq \delta$.

Для доказательства следствия необходимо отметить, что $\Delta_{T,0}^{\alpha_1, \beta_1} = \Delta_{T,1}^{\alpha_1, \beta_1}$ для всех $\alpha_1, \beta_1 \in \mathbb{F}_2^{n-1}$. Тогда, согласно следствию 1, задача построения дифференциальной 2δ -равномерных подстановок сводится к поиску двух подстановок $\pi_0, \pi_1 \in \mathbb{S}(\mathbb{F}_2^{n-1})$, таких, что количество решений уравнений

$$\pi_0(x) + \pi_1(x + \alpha_1) = \beta_1 \quad (2)$$

при всевозможных значениях $\alpha_1, \beta_1 \in \mathbb{F}_2^{n-1}$ не больше 2. Действительно, если $T(x_1, i) = \pi_i(x_1)$, $i \in \{0, 1\}$, $U(x_2, x_1)$ — линейная по x_2 функция при произвольной фиксации x_1 , то с использованием формулы (1) получим подстановку с показателем дифференциальной равномерности 2δ . В качестве π_0, π_1 можно взять произвольную дифференциальную 2 -равномерную подстановку. В этом случае, с учётом следствия 1 и замечания 1, функция F является подстановкой с показателем дифференциальной равномерности большим либо равным 4. При этом если максимальное количество решений (2) равно двум, то подстановка будет дифференциальной 4 -равномерной, иначе показатель её дифференциальной равномерности будет определяться удвоенным максимальным количеством решений уравнений вида (2).

Теорема 2. Пусть $x_1 \in \mathbb{F}_{2^{n-1}}$, n чётное, $n > 6$, $x_2 \in \mathbb{F}_2$, f — произвольная булева функция от $n - 1$ переменной, $c \in \mathbb{F}_{2^{n-1}} \setminus \{\mathbf{0}, \mathbf{1}\}$,

$$\begin{aligned} T: \mathbb{F}_{2^{n-1}} \times \mathbb{F}_2 &\rightarrow \mathbb{F}_{2^{n-1}}, & T(x_1, x_2) &= x_1^{-1} \cdot c^{x_2}, \\ U: \mathbb{F}_2 \times \mathbb{F}_{2^{n-1}} &\rightarrow \mathbb{F}_2, & U(x_2, x_1) &= f(x_1) + x_2. \end{aligned}$$

Тогда формула (1) задаёт подстановку F , при этом

- 1) если $\text{tr}(c) = \text{tr}(c^{-1}) = 1$, то $\delta_F = 4$;
- 2) иначе $\delta_F = 6$.

Замечание 2. Результат п. 1 теоремы 2 доказан в [8], однако следствие 1 позволяет проводить доказательство с более общих позиций.

Теорема 3. Пусть $x_1 \in \mathbb{F}_{2^{n-1}}$, n чётное, $n > 6$, $x_2 \in \mathbb{F}_2$, f — произвольная булева функция от $n - 1$ переменной, $c \in \mathbb{F}_{2^{n-1}} \setminus \{\mathbf{0}, \mathbf{1}\}$,

$$\begin{aligned} T: \mathbb{F}_2^{n-1} \times \mathbb{F}_2 &\rightarrow \mathbb{F}_2^{n-1}, & T(x_1, x_2) &= x_1^3 \cdot c^{x_2}, \\ U: \mathbb{F}_2 \times \mathbb{F}_{2^{n-1}} &\rightarrow \mathbb{F}_2, & U(x_2, x_1) &= f(x_1) + x_2. \end{aligned}$$

Тогда формула (1) задаёт подстановку F , при этом $\delta_F = 6$.

Напомним, что две (n, m) -функции g и f называются расширенно аффинно-эквивалентными, если существуют аффинные подстановки a и b пространств \mathbb{F}_2^n и \mathbb{F}_2^m соответственно и аффинная (n, m) -функция c , что $f(x) = (b \circ g \circ a)(x) + c(x)$ [1]. Расширенно аффинно-эквивалентные функции, очевидно, имеют одинаковый показатель дифференциальной равномерности. В доказательстве теоремы 3 используется тот факт, что уравнение третьей степени не может иметь больше трёх решений. Естественно предположить, что если взять в качестве $T(x_1, i) = x_1^3 + a_i x_1^2 + b_i x_1$ — функции, расширенно аффинно-эквивалентные 2-равномерной подстановке x^3 , то можно построить 4-равномерные подстановки F с использованием формулы (1). Следующее утверждение показывает, что это не так.

Утверждение 1. Пусть $x_1 \in \mathbb{F}_{2^{n-1}}$, n чётное, $n > 6$, $x_2 \in \mathbb{F}_2$, f — произвольная булева функция от $n - 1$ переменной, $a, b \in \mathbb{F}_{2^{n-1}}$,

$$\begin{aligned} T: \mathbb{F}_2^{n-1} \times \mathbb{F}_2 &\rightarrow \mathbb{F}_2^{n-1}, \quad T(x_1, 0) = x_1^3, \quad T(x_1, 1) = x_1^3 + a \cdot x_1^2 + b \cdot x_1, \\ U: \mathbb{F}_2 \times \mathbb{F}_2^{n-1} &\rightarrow \mathbb{F}_2, \quad U(x_2, x_1) = f(x_1) + x_2. \end{aligned}$$

Тогда существуют $\alpha_1, \beta_1 \in \mathbb{F}_{2^{n-1}}$, такие, что количество решений уравнения $T(x_1 + \alpha_1, 0) + T(x_1, 1) = \beta_1$ равно 2^{n-1} , либо $T(x_1, 1)$ не является подстановкой.

Приведём ещё несколько результатов, полученных применением теоремы 1.

Утверждение 2. Пусть $x_1 \in \mathbb{F}_{2^{n-1}}$, n чётное, $n > 6$, $x_2 \in \mathbb{F}_2$, f — произвольная булева функция от $n - 1$ переменной,

$$\begin{aligned} T: \mathbb{F}_{2^{n-1}} \times \mathbb{F}_2 &\rightarrow \mathbb{F}_{2^{n-1}}, \quad T(x_1, 0) = x_1^3, \quad T(x_1, 1) = x_1^{-1}, \\ U: \mathbb{F}_2^1 \times \mathbb{F}_2^{n-1} &\rightarrow \mathbb{F}_2, \quad U(x_2, x_1) = f(x_1) + x_2. \end{aligned}$$

Тогда формула (1) задаёт подстановку F , при этом $\delta_F = 8$.

Утверждение 3. Пусть $t = 2$, $x_1 \in \mathbb{F}_2^{n-t}$, $x_2 \in \mathbb{F}_2^t$. Тогда существуют такие c_{x_2} , $x_2 \in \mathbb{F}_{2^2}$, $c_{x'_2} \neq c_{x''_2}$ при $x'_2 \neq x''_2$, что подстановка F , задаваемая формулой (1), дифференциально 8-равномерна, где

$$\begin{aligned} T: \mathbb{F}_2^{n-t} \times \mathbb{F}_2^t &\rightarrow \mathbb{F}_2^{n-1}, \quad T(x_1, x_2) = x_1^{-1} \cdot c_{x_2}, \\ U: \mathbb{F}_2^t \times \mathbb{F}_2^{n-t} &\rightarrow \mathbb{F}_2^t, \text{ при фиксации произвольного } x_1 \text{ функция } U(x_2, x_1) \text{ является подстановкой по переменной } x_2. \end{aligned}$$

ЛИТЕРАТУРА

1. Canteaut A. and Perrin L. On CCZ-Equivalence, Extended-Affine Equivalence, and Function Twisting. Cryptology ePrint Archive: Report 2018/713.
2. Biryukov A., Perrin L., and Udovenko A. Reverse-engineering the S-box of Streebog, Kuznyechik and Stribobr1 // LNCS. 2016. V. 9665. P. 372–402.
3. Biryukov A., Perrin L., and Udovenko A. Cryptanalysis of a Theorem: Decomposing the Only Known Solution to the Big APN Problem (Full Version). Cryptology ePrint Archive: Report 2016/539.
4. De la Cruz Jiménez R. A. Generation of 8-bit S-Boxes Having Almost Optimal Cryptographic Properties Using Smaller 4-bit S-Boxes and Finite Field Multiplication. 2017. www.cs.haifa.ac.il/orrd/LC17/paper60.pdf.
5. Fomin D. B. New classes of 8-bit permutations based on a butterfly structure // Матем. вопр. криптогр. 2019. Т. 10. № 2. С. 169–180.
6. Фомин Д. Б. Построение подстановок пространства V_{2m} с использованием $(2m, m)$ -функций. // Матем. вопр. криптогр. 2020. Т. 11. № 3. С. 121–138.

7. Фомин Д. Б. Об алгебраической степени и дифференциальной равномерности подстановок пространства V_{2m} , построенных с использованием $(2m, m)$ -функций. // Матем. вопр. криптогр. 2020. Т. 11. № 4. С. 133–149.
8. Carlet C., Tang D., Tang X., and Liao Q. New construction of differentially 4-uniform bijections // LNCS. 2013. V. 8567. P. 22–38.

УДК 519.719.325

DOI 10.17223/2226308X/14/10

УСЛОВИЕ ОДНОЗНАЧНОСТИ РАЗЛОЖЕНИЯ В ПРОИЗВЕДЕНИЕ ФУНКЦИЙ p -ЗНАЧНОЙ ЛОГИКИ ПРИ ЛИНЕЙНОЙ ЗАМЕНЕ ПЕРЕМЕННЫХ

А. В. Черемушкин

Рассматривается множество разложений функции p -значной логики в произведение функций от непересекающихся множеств переменных при различных линейных преобразованиях аргументов. Каждому такому разложению соответствует разложение векторного пространства в прямую сумму подпространств. Приведены условия, при которых разложение определяется однозначно с точностью до перестановки подпространств между собой.

Ключевые слова: двоичные функции, разложение в прямую сумму, линейное преобразование.

Пусть $n \geq 1$, $V_n = \mathbb{Z}_p^n$ рассматривается как векторное пространство над полем \mathbb{Z}_p , $\mathcal{F}_n = \{f : V_n \rightarrow \mathbb{Z}_p\}$ — множество функций от n переменных.

Пусть $1 \leq k \leq n$. Говорят, что переменные x_{k+1}, \dots, x_n функции $f(x_1, \dots, x_n)$ являются несущественными, если найдётся функция $h(x_1, \dots, x_k)$, такая, что $f = h$. Нетрудно видеть, что переменная x_n является несущественной для функции f , если и только если $f(x + e^n) = f(x)$ при $e^n = (0, \dots, 0, 1)$.

Пусть $(\mathbf{H}_n)_f$ — группа инерции функции f в группе сдвигов \mathbf{H}_n , т. е. множество таких сдвигов $\begin{pmatrix} x \\ x+a \end{pmatrix} \in \mathbf{H}_n$, что выполнено сравнение $f(x+a) = f(x)$, $x \in V_n$.

Условие тривиальности группы инерции $(\mathbf{H}_n)_f$ равносильно тому, что у всех функций, полученных из f всевозможными линейными заменами переменных, все переменные будут существенными.

Назовём носителем функции $f : V_n \rightarrow \mathbb{Z}_p$ множество векторов, на которых она принимает ненулевые значения:

$$f^{-1}(*) = \{a \in V_n : f(a) \neq 0\}.$$

Если носитель функции содержится в некотором многообразии размерности k , то это позволяет сводить задачу исследования функции от n переменных к задаче исследования функции от $n - k$ переменных.

Лемма 1. Пусть функция $f : V_n \rightarrow \mathbb{Z}_p$ не является константой. Если носитель $f^{-1}(*)$ функции f содержится в многообразии $L + a \subset V_n$, $1 \leq \dim L \leq n - 1$, то существует линейное преобразование A пространства V_n , функция $h : \mathbb{Z}_p^{n-k} \rightarrow \mathbb{Z}_p$ и элементы $a_1, \dots, a_k \in \mathbb{Z}_p$, $k = n - \dim L$, такие, что функцию $f(xA)$ можно представить в виде

$$f(xA) = J_{a_1}(x_1) \dots J_{a_k}(x_k)h(x_{k+1}, \dots, x_n),$$