МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.719.2 DOI 10.17223/20710410/57/1

ОБ ЭВРИСТИЧЕСКОМ АЛГОРИТМЕ ПОСТРОЕНИЯ ПОДСТАНОВОК С ЗАДАННЫМИ КРИПТОГРАФИЧЕСКИМИ ХАРАКТЕРИСТИКАМИ С ИСПОЛЬЗОВАНИЕМ ОБОБЩЁННОЙ КОНСТРУКЦИИ

М. А. Коврижных, Д. Б. Фомин

Национальный исследовательский университет «Высшая школа экономики», г. Москва, Россия

E-mail: makovrizhnykh@gmail.com, dfomin@hse.ru

Исследована возможность построения с помощью обобщённой конструкции подстановок с заданными криптографическими характеристиками, обеспечивающими стойкость алгоритмов шифрования к линейному и разностному методам криптоанализа. Предложен эвристический алгоритм поиска параметров обобщённой конструкции, полученных посредством умножения на транспозиции. Используются идеи генетического алгоритма, спектрально-линейного и спектрально-разностного методов. Изучены вопросы оптимизации вычисления криптографических характеристик на каждой итерации алгоритма. Экспериментальные исследования наиболее интересных с практической точки зрения 8-битовых подстановок показали, что можно построить 6-равномерные подстановки с нелинейностью 108.

Ключевые слова: *векторная булева функция, подстановка, дифференциальная δ-равномерность, нелинейность.*

HEURISTIC ALGORITHM FOR OBTAINING PERMUTATIONS WITH GIVEN CRYPTOGRAPHIC PROPERTIES USING A GENERALIZED CONSTRUCTION

M. A. Kovrizhnykh, D. B. Fomin

National Research University Higher School of Economics, Moscow, Russia

In this paper, we study a generalized construction of $(2m, 2m)$-functions using monomial and arbitrary m-bit permutations as constituent elements. We investigate the possibility of constructing bijective vectorial Boolean functions (permutations) with specified cryptographic properties that ensure the resistance of encryption algorithms to linear and differential methods of cryptographic analysis. We propose a heuristic algorithm for obtaining permutations with the given nonlinearity and differential uniformity based on the generalized construction. For this purpose, we look for auxiliary permutations of a lower dimension using the ideas of the genetic algorithm, spectral-linear, and spectral-difference methods. In the case of $m = 4$, the proposed algorithm consists of iterative multiplication of the initial randomly generated 4-bit

permutations by transposition, selecting the best ones in nonlinearity, the differential uniformity, and the corresponding values in the linear and differential spectra among the obtained 8-bit permutations. We show how to optimize the calculation of cryptographic properties at each iteration of the algorithm. Experimental studies of the most interesting, from a practical point of view, 8-bit permutations have shown that it is possible to construct 6-uniform permutations with nonlinearity 108.

Keywords: *vectorial Boolean function, permutation, differential uniformity, nonlinearity.*

Введение

Конструирование алгоритмов шифрования, стойких к известным методам анализа, представляет собой один из главных аспектов защиты информации. Среди наиболее исследуемых методов криптографического анализа выделим линейный и разностный методы.

Разностный криптоанализ был представлен научной общественности в 1990 г. Э. Бихамом и А. Шамиром [1, 2]. Этот метод использует наличие высоковероятного разностного соотношения на определённых раундах шифрования, вероятность выполнения которого не зависит от ключа. Под разностью будем понимать результат побитового сложения n-мерных векторов. Знание наиболее вероятных разностных соотношений даёт возможность использовать материал для восстановления битов раундового ключа.

Линейный криптоанализ впервые описан в 1993 г. М. Мацуи [3]. Метод применим при наличии высоковероятного линейного статистического аналога для определённых раундов шифрования. Аналогично разностному методу, некоторые раунды шифрования можно заменить их линейным аналогом, который, независимо от ключа, выполняется с вероятностью p для случайно заданного открытого текста и соответствующего ему шифртекста выделенной части шифра. Наибольшее отклонение p от $1/2$ определяет эффективность найденного линейного выражения. С использованием построенного эффективного линейного статистического аналога производится отбраковывание ложных ключей.

Векторные булевы функции — одни из основных примитивов современных симметричных шифров, обеспечивающих свойство перемешивания [4], — должны иметь криптографические характеристики, гарантирующие неосуществимость применения разностного и линейного методов криптографического анализа. Так, векторные булевы функции с высокой нелинейностью позволяют гарантировать стойкость к линейному анализу, поскольку их не удастся эффективно заменить линейным аналогом той же размерности. Для конструирования криптографических алгоритмов, стойких к разностному анализу, используют функции с минимально возможным показателем дифференциальной δ-равномерности.

Дополнительно, векторные булевы функции, используемые в блочных шифрах, как правило, должны быть биективными для обеспечения однозначного расшифрования, т. е. подстановками. В современных криптографических алгоритмах ГОСТ 34.12-2018 («Кузнечик»), AES, ARIA, Khazad и других 8-битовые подстановки являются единственными нелинейными элементами конструкции. Полный перебор $(8, 8)$-функций в настоящее время нереализуем. Таким образом, получение подстановок размерности $n \geqslant 8$ бит с заданными криптографическими свойствами, лучшими, чем у псевдослучайно сгенерированных, и допускающих эффективную аппаратную реализацию,

является сложной и актуальной задачей, что подтверждается большим количеством новейших научных публикаций и докладов на всероссийских и международных конференциях, посвященных данной тематике [5 – 15].

Известные подходы к построению подстановок могут быть разделены на явные алгебраические методы, псевдослучайное генерирование и эвристические подходы (см., например, обзор в [5]). Перспективной представляется идея комбинации этих подходов, в частности использование функциональных схем для получения подстановок с помощью функций меньшей размерности (см. обзор в [11]). При этом в таких схемах обычно есть некоторые параметры, подходящим выбором которых можно улучшить криптографические характеристики конструируемых подстановок.

Так, в работе [6] описана конструкция, содержащая инверсию в поле $\mathbb{F}_{2^4}$ и две произвольные подстановки пространства V_4, для построения 8-битовых подстановок со значениями нелинейности до 108, показателя дифференциальной δ-равномерности 6 или 8, алгебраической степени 7, алгебраической иммунности 3.

В работах [7, 8] представлены схемы, основанные на известных структурах Фейстеля и Лея — Месси, для генерации подстановок размерности $n = 2k$, $k > 2$. Предложенные конструкции используют инверсию в поле $\mathbb{F}_{2^k}$, произвольную k-битовую небиективную функцию (которая не имеет прообраза для 0) и любую k-битовую подстановку. Комбинируя эти компоненты с умножением в конечном поле, автор представил новые 8-битовые подстановки без фиксированных точек, обладающие таким же сочетанием криптографических свойств, как и в [6]. В [8] показано, что такой подход может быть использован для построения инволюций и ортоморфизмов с хорошими криптографическими характеристиками. Однако в этих работах не приведено теоретического обоснования выбора предложенных конструкций.

В работе [10] предложены новые классы 8-битовых подстановок, основанные на конструкции типа «бабочка». Показано, что существует не менее 36 новых конструкций подстановок, которые имеют нелинейность 108, показатель дифференциальной δ-равномерности 6, минимальную степень 7 и значение алгебраической иммунности 3 и могут быть эффективно реализованы как программно, так и аппаратно.

Работы [9, 11, 12] распространяют способы построения подстановок из [10] на случай произвольного векторного пространства V_{2m} и теоретически обосновывают полученные в них экспериментальные результаты. В качестве функциональной схемы используется TU-представление, описанное в [16, 17]. Доказаны необходимые, а в некоторых случаях и достаточные условия для того, чтобы результирующая подстановка обладала заданными значениями нелинейности, алгебраической степени и показателя дифференциальной δ-равномерности. Описана новая обобщённая конструкция векторных функций, использующая мономиальные подстановки в качестве основных составляющих элементов. В случае $m = 4$ экспериментально найдены 768 наборов параметров обобщённой конструкции, с использованием которых при правильном выборе вспомогательных 4-битовых подстановок получены 8-битовые 6-равномерные подстановки, имеющие нелинейность 108 и минимальную степень 7.

Остановимся кратко на методах, относящихся к эвристическому подходу и основанных на итеративном улучшении характеристик подстановок.

В [18] предложен усовершенствованный метод градиентного спуска для построения векторных булевых функций с хорошим сочетанием криптографических свойств. Так, 8-битовые подстановки, полученные этим методом, имеют нелинейность 104, показатель дифференциальной δ-равномерности 8, минимальную степень 7.

Используя обратный генетический алгоритм для генерации подстановок размерности от 8×8 до 16×16, авторы работы [15] для случая 8-битовых подстановок достигли значений нелинейности от 106 до 112 при показателе дифференциальной δ-равномерности 6.

В работе [5] представлены методы итеративного улучшения криптографических характеристик подстановки посредством её умножения на транспозиции — спектрально-линейный и спектрально-разностный методы, основанные на использовании линейного и разностного спектров. В результате применения этих методов удалось получить большое количество 8-битовых подстановок со следующими криптографическими свойствами: нелинейность 104, показатель дифференциальной δ-равномерности 6, обобщённая минимальная степень 7.

Целью настоящей работы является исследование возможности построения подстановок с заданными криптографическими характеристиками — дифференциальной δ-равномерностью и нелинейностью — посредством умножения на транспозиции вспомогательных подстановок в обобщённой конструкции.

В п. 1 приводятся основные определения и обозначения, используемые в работе, в п. 2 рассмотрена обобщённая конструкция $(2m, 2m)$-функции. В п. 3 идеи генетического алгоритма, спектрально-линейного и спектрально-разностного методов применены для выбора подстановок меньшей размерности в обобщённой конструкции. Предложен алгоритм, в результате реализации которого построены 6-равномерные 8-битовые подстановки с нелинейностью 108 и минимальной степенью 7. Обоснованы утверждения, в которых исследуются изменения в DDT и LAT подстановок, задаваемых обобщённой конструкцией, при умножении вспомогательных подстановок на транспозиции.

1. Основные определения и обозначения

Обозначим через V_n, $n \in \mathbb{N}$, n-мерное векторное пространство над полем из двух элементов $\mathbb{F}_2$, $V_n^\times = V_n \setminus \{0\}$. Конечное поле из 2^n элементов обозначим через $\mathbb{F}_{2^n}$. Здесь $\mathbb{F}_{2^n} = \mathbb{F}_2[x]/g(x)$, где $g(x)$ — некоторый неприводимый многочлен степени n над полем $\mathbb{F}_2$; $\mathbb{Z}/2^n$ — кольцо целых чисел по модулю 2^n. Существуют взаимно-однозначное отображение $\mathbb{Z}/2^n \to V_n$, ставящее в соответствие элементу кольца $\mathbb{Z}/2^n$ его двоичное представление, и взаимно-однозначное отображение $V_n \to \mathbb{F}_{2^n}$, ставящее в соответствие двоичной строке элемент поля $\mathbb{F}_{2^n}$, определённые следующим образом:

$$a_{n-1}2^{n-1} + \ldots + a_0 \;\leftrightarrow\; (a_{n-1}, \ldots, a_0) \;\leftrightarrow\; a_{n-1}x^{n-1} + \ldots + a_0.$$

Операции сложения и умножения в поле $\mathbb{F}_{2^n}$ будем обозначать знаками «$+$» и «$\cdot$» соответственно.

Пусть $a \in V_n$, $b \in V_m$. *Конкатенацию* двух векторов обозначим через $a\|b \in V_{n+m}$. *Скалярным произведением* двух векторов $a, b \in V_n$ называется элемент поля $\mathbb{F}_2$, вычисляемый по формуле $\langle a, b\rangle = a_{n-1}b_{n-1} + \ldots + a_0b_0$, где сложение и умножение проводятся в поле $\mathbb{F}_2$. Заметим, что прямое произведение векторных пространств $V_m \times V_m$ можно ассоциировать с V_{2m}.

Определение 1. Пусть n и m — натуральные числа. *Векторной булевой (n, m)-функцией* F называется отображение $F : V_n \to V_m$. При $m = 1$ говорят, что F — *булева функция* от n переменных.

Каждая булева функция f от n переменных единственным образом представляется в виде *полинома Жегалкина* — многочлена от n переменных над полем $\mathbb{F}_2$, в котором

каждая переменная входит в каждый моном в степени 0 или 1. При этом под *алгебраической степенью* (она обозначается как $\deg(f)$) булевой функции f понимается максимальная степень монома с коэффициентом, отличным от 0.

Векторная булева (n, m)-функция F однозначно задается набором своих *координатных* булевых функций от n переменных: $F = (f_{m-1}, \ldots, f_0)$; *компонентной* функцией называется любая ненулевая линейная комбинация координатных функций, т. е. $\langle a, F(x)\rangle$, где $a \in V_m^\times$.

Определение 2. *Подстановкой пространства* V_n называется биективная (n, n)-функция.

Симметрическую группу всех подстановок пространства V_n обозначим $S(V_n)$. Одним из способов представления подстановок является таблица из двух строк: первая строка содержит все числа от 0 до $2^n - 1$, а вторая — образы соответствующих элементов первой строки.

Определение 3. *Мономиальные* подстановки поля $\mathbb{F}_{2^m}$ — это подстановки вида x^d, где d — такое положительное целое число, что $(d, 2^m - 1) = 1$.

При этом можно рассматривать только значения $d < 2^m - 1$. В частности, при $m = 4$ мономиальные подстановки получаются при $d \in \{1, 2, 4, 7, 8, 11, 13, 14\}$. При этом линейными мономиальными подстановками поля $\mathbb{F}_{2^4}$ являются x^d при $d \in \{1, 2, 4, 8\}$ [19, с. 72, 74].

Определение 4. *Циклической подстановкой* (*циклом*) называется подстановка, переводящая j_1 в j_2, j_2 — в j_3, …, j_{k-1} — в j_k и j_k — в j_1. Такой цикл кратко записывается в виде $(j_1, j_2, \ldots, j_k)$. *Транспозиция* — это цикл длины 2, т. е. подстановка, оставляющая неподвижными все элементы, за исключением двух, которые меняются местами.

Умножение подстановки F на транспозицию слева $(j_1, j_2) \circ F$ приводит к транспозиции элементов j_1 и j_2 в нижней строке подстановки F [20, с. 51]:

$$(j_1, j_2) \circ \begin{pmatrix} 0 & 1 & i_1 & \ldots & i_2 & \ldots & 2^n - 1 \\ F(0) & F(1) & F(i_1) = j_1 & \ldots & F(i_2) = j_2 & \ldots & F(2^n - 1) \end{pmatrix} =$$
$$= \begin{pmatrix} 0 & 1 & i_1 & \ldots & i_2 & \ldots & 2^n - 1 \\ F(0) & F(1) & j_2 = F(i_2) & \ldots & j_1 = F(i_1) & \ldots & F(2^n - 1) \end{pmatrix}.$$

Умножение подстановки F на транспозицию справа $F \circ (i_1, i_2)$ приводит к транспозиции элементов i_1 и i_2 в верхней строке подстановки F, другими словами, в нижней строке подстановки F меняются местами образы элементов i_1 и i_2.

Определение 5. *Индикаторной функцией* $I_b(x)$ для $b, x \in V_n$ называется функция

$$I_b(x) = \begin{cases} 1, & b = x, \\ 0, & b \neq x. \end{cases}$$

Приведём определения некоторых криптографических характеристик булевых (n, n)-функций.

Определение 6. Говорят, что (n, n)-функция F является *дифференциально* δ_F*-равномерной*, если

$$\delta_F = \max_{a \in V_n^\times, b \in V_n} \delta_F(a, b),$$

где

$$\delta_F(a, b) = |\{x \in V_n : F(x + a) + F(x) = b\}|.$$

Значение δ_F называется *показателем дифференциальной равномерности* функции F.

Использование функций с малым показателем дифференциальной равномерности при синтезе криптографических алгоритмов позволяет повысить стойкость к разностному методу криптоанализа. Наименьшее возможное значение δ_F равно 2, при этом известен только один пример (с точностью до CCZ-эквивалентности) взаимно-однозначной 2-равномерной (n,n)-функции для чётных n — 6-битная подстановка Диллона [21]. Для случая $n=8$ большим значением показателя дифференциальной δ-равномерности будем считать $\delta_F > 8$, поскольку 8-битовую подстановку с $\delta_F = 8$ можно получить псевдослучайным поиском [5, 22, 23].

Определение 7. *Таблицей распределения разностей* (Difference Distribution Table — DDT) (n,n)-функции F называется такая $2^n \times 2^n$ таблица DDT_F, что

$$\mathrm{DDT}_F[a,b] = \delta_F(a,b).$$

Для всех элементов $\delta \in \{0,2,\ldots,2^n\}$ определим множества

$$D_F(\delta) = \{(a,b) \in V_n^\times \times V_n : \delta_F(a,b) = \delta\}.$$

Определение 8. *Разностным спектром* (n,n)-функции F называется множество пар

$$D_F = \{(\delta, |D_F(\delta)|)\}.$$

Определение 9. *Преобразованием Уолша — Адамара* $W_F(a,b)$ (n,n)-функции F называется отображение $W_F : V_n \times V_n \to \mathbb{Z}$, заданное равенством

$$W_F(a,b) = \sum_{x \in V_n} (-1)^{\langle a,x\rangle + \langle b,F(x)\rangle} \quad \text{для любых} \quad a,b \in V_n.$$

Определение 10. *Линейность* ℓ_F (n,n)-функции F определяется следующим образом:

$$\ell_F = \max_{a \in V_n,\, b \in V_n^\times} |W_F(a,b)|.$$

Нелинейностью N_F (n,n)-функции F называется величина, вычисляемая по формуле

$$N_F = 2^{n-1} - \frac{1}{2}\ell_F.$$

Использование функций с большей нелинейностью при синтезе криптографических алгоритмов позволяет повысить стойкость к линейному методу криптографического анализа.

Определение 11. *Таблицей линейных приближений* (Linear Approximation Table — LAT) [24] (n,n)-функции F называется такая $2^n \times 2^n$ таблица LAT_F, что

$$\mathrm{LAT}_F[a,b] = \ell_F(a,b),$$

где

$$\ell_F(a,b) = \big|\{x \in V_n : \langle a,x\rangle = \langle b,F(x)\rangle\}\big| - 2^{n-1} = \frac{1}{2}W_F(a,b).$$

Для всех элементов $\ell \in \{0,2,\ldots,2^{n-1}\}$ определим множества

$$L_F(\ell) = \{(a,b) \in V_n \times V_n^\times : \big|\ell_F(a,b)\big| = \ell\}.$$

Определение 12. *Линейным спектром* (n,n)-функции F называется множество пар

$$L_F = \{(\ell, |L_F(\ell)|)\}.$$

Определение 13. *Минимальной степенью* (n,n)-функции F называется минимальная из алгебраических степеней всех компонентных функций [25, 2.2.1], т. е.

$$\deg_{\min}(F) = \min_{a \in V_n^\times} \deg(\langle a, F(x)\rangle).$$

Подстановки, используемые в блочных шифрах, должны иметь высокую минимальную степень, чтобы обеспечивать стойкость, например, к разностной атаке высоких порядков. Для подстановок $F \in S(V_n)$ максимально возможная минимальная степень равна $n-1$ [25].

2. Обобщённая конструкция $(2m,2m)$-функции

Пусть $(2m,2m)$-функция $F(x_1,x_2) = y_1 \| y_2$, где $x_1, x_2, y_1, y_2 \in V_m$, задаётся следующей *обобщённой* конструкцией, впервые введённой в работе [9]:

$$\begin{aligned} y_1 = F_1(x_1,x_2) &= \begin{cases} x_1^\alpha \cdot x_2^\beta, & x_2 \neq 0, \\ \widehat{\pi}_1(x_1), & x_2 = 0, \end{cases} \\ y_2 = F_2(x_1,x_2) &= \begin{cases} x_1^\gamma \cdot x_2^\delta, & x_1 \neq 0, \\ \widehat{\pi}_2(x_2), & x_1 = 0. \end{cases} \end{aligned} \tag{1}$$

Здесь следует перейти от m-мерных векторов к соответствующим элементам поля $\mathbb{F}_{2^m}$ и выполнить возведение в степень и умножение в поле $\mathbb{F}_{2^m}$. Кроме того, в (1) $\widehat{\pi}_1$, $\widehat{\pi}_2$ — подстановки пространства V_m. Без ограничения общности будем предполагать, что

$$\widehat{\pi}_1(0) = 0, \quad \widehat{\pi}_2(0) = 0. \tag{2}$$

Параметрами функции (1) являются набор показателей степеней $(\alpha,\beta,\gamma,\delta)$ мономиальных подстановок и значения подстановок $\widehat{\pi}_1, \widehat{\pi}_2 \in S(V_m)$.

Отметим, что конструкция (1) основана на структуре типа «бабочка», введённой в [16] и полученной при изучении декомпозиции APN-подстановки Диллона [21], и допускает TU-представление [17].

В работе [14] для $m = 4$ на множестве всех 4096 наборов показателей степеней $(\alpha,\beta,\gamma,\delta)$ мономиальных подстановок введено отношение эквивалентности и получено разбиение этого множества на непересекающиеся классы. Обоснованы утверждения, позволяющие по одному представителю класса эквивалентности отбраковать все функции, определяемые наборами из данного класса, либо по высокому показателю дифференциальной δ-равномерности ($\delta_F \geqslant 14$), либо вследствие того, что они не являются подстановками ни при каких значениях вспомогательных подстановок $\widehat{\pi}_1$, $\widehat{\pi}_2$. В результате остались неотбракованными 768 наборов параметров $(\alpha,\beta,\gamma,\delta)$, перспективных для использования в конструкции (1) с целью получения 8-битовых подстановок с достаточно низким показателем дифференциальной δ-равномерности.

3. О подборе подстановок $\widehat{\pi}_1$, $\widehat{\pi}_2$ в обобщённой конструкции

Далее будем рассматривать обобщённую конструкцию (1) в случае $m = 4$ с одним из 768 наборов параметров $(\alpha,\beta,\gamma,\delta)$, описанных в [9, 12, 14]. Отметим, что вспомогательные подстановки $\widehat{\pi}_1, \widehat{\pi}_2$ в (1) выбираются независимо от параметров $(\alpha,\beta,\gamma,\delta)$.

Дадим эвристический алгоритм поиска таких вспомогательных 4-битовых подстановок, чтобы итоговая 8-битовая подстановка обладала заданными криптографическими характеристиками $N_F = 108$, $\delta_F = 6$; при этом используем идеи генетического алгоритма, спектрально-линейного и спектрально-разностного методов [5].

3.1. О подборе вспомогательных 4-битовых подстановок

Кратко суть предлагаемого алгоритма 1 заключается в последовательном умножении 4-битовых подстановок $\widehat{\pi}_1$ или $\widehat{\pi}_2$ на транспозиции и отборе среди полученных по формулам (1) 8-битовых подстановок лучших по нелинейности, показателю дифференциальной равномерности и соответствующим значениям в линейном и разностном спектрах. Таким образом, текущее поколение из Num_Best пар подстановок $(\widehat{\pi}_1, \widehat{\pi}_2)$ порождает $Num\_Best \cdot Num\_Trans$ новых пар, из них «выживают» только Num_Best лучших. При этом скрещивания не производится, только «случайные мутации» внутри $\widehat{\pi}_1$ (или $\widehat{\pi}_2$).

Алгоритм 1.

Вход: Подстановка $F \in S(V_8)$, построенная по формулам (1) с использованием одного из 768 наборов параметров $(\alpha, \beta, \gamma, \delta)$ [12] и произвольных 4-битовых подстановок $\widehat{\pi}_1$, $\widehat{\pi}_2$ (2), с криптографическими характеристиками $\ell_F > 40$ или $\delta_F > 6$.

Параметры: Num_Trans — количество умножений на транспозиции; Num_Best — количество отбираемых пар $(\widehat{\pi}_1, \widehat{\pi}_2)$ на каждой итерации алгоритма.

1: Сформировать список $Best$ из одной пары подстановок $(\widehat{\pi}_1, \widehat{\pi}_2)$.
2: **Для всех** пар подстановок $(\widehat{\pi}_1, \widehat{\pi}_2)$ из списка $Best$:
3: запомнить пару $(\widehat{\pi}_1, \widehat{\pi}_2)$ как просмотренную;
4: псевдослучайно выбрать номер $t \in \{1, 2\}$.
5: **Для** $i = 1, \ldots, Num\_Trans$
6: псевдослучайно выбрать $x, y \in V_4^{\times}$, $x \neq y$, получить подстановку $\widehat{\pi}_t = \widehat{\pi}_t \circ (x, y)$.
7: **Если** пара $(\widehat{\pi}_1, \widehat{\pi}_2)$ ещё не просмотрена, **то**
8: встроить $\widehat{\pi}_t$ в F;
9: вычислить набор характеристик подстановки (ℓ_F, δ_F, $|L_F(\ell_F/2)|$, $|D_F(\delta_F)|$);
10: добавить пару $(\widehat{\pi}_1, \widehat{\pi}_2)$ в список $Best$.
11: Отобрать (по принципу многоуровневой сортировки по возрастанию) Num_Best лучших (т. е. с меньшими значениями с учётом приоритетов) из всех наборов характеристик подстановок F, порождённых парами $(\widehat{\pi}_1, \widehat{\pi}_2)$ из текущего списка $Best$, считая, что в наборе приоритет убывает от ℓ_F к $|D_F(\delta_F)|$.
12: **Если** в наилучшем наборе значения $\ell_F = 40$ и $\delta_F = 6$, **то**
вывести подстановки $\widehat{\pi}_1, \widehat{\pi}_2$, порождающие подстановку F,
13: **иначе**
14: сформировать новый список $Best$ из Num_Best пар подстановок $(\widehat{\pi}_1, \widehat{\pi}_2)$, соответствующих лучшим наборам, отобранным на шаге 11.
15: **Перейти** к шагу 2.

Выход: Подстановка $F \in S(V_8)$, отличающаяся от исходной только значениями подстановок $\widehat{\pi}_1$, $\widehat{\pi}_2$, такая, что

$$\ell_F = 40 \quad \big(N_F = 108\big), \qquad \delta_F = 6. \tag{3}$$

Значения Num_Trans, Num_Best являются входными данными алгоритма 1. Вычислительные эксперименты показали, что при $Num\_Trans = 500$ на первой итерации (размер начальной популяции), $Num\_Trans = 100$ на последующих, и при $Num\_Best = 10$ за приемлемое число итераций получаются 8-битовые подстановки с характеристиками (3) и минимальной степенью 7. Вопрос о возможности получения с использованием конструкции (1) подстановок с $N_F > 108$, $\delta_F \leqslant 6$ требует дополнительного исследования.

3.2. Об изменениях некоторых криптографических характеристик при умножении на транспозицию вспомогательных 4-битовых подстановок

В [26] доказано, что при умножении векторной булевой функции на транспозицию показатель её дифференциальной равномерности и нелинейность изменяются незначительно, в частности обоснованы следующие оценки: для $h = g \circ (x, y)$, таких, что $g, h : V_n \to V_n$, выполняется

$$\delta_h - 4 \leqslant \delta_g \leqslant \delta_h + 4; \tag{4}$$

$$N_h - 2 \leqslant N_g \leqslant N_h + 2. \tag{5}$$

В работе [13] обоснованы подходы к сокращению трудоёмкости вычисления разностного и линейного спектров для подстановки, полученной умножением исходной на одну транспозицию, в частности показано, что изменения в DDT появляются в относительно небольшом числе ячеек, а именно: в каждой строке таблицы, начиная с первой, возможны изменения не более чем в четырёх ячейках. Тем самым предложенный в [13] алгоритм пересчёта разностного спектра и, как следствие, показателя дифференциальной равномерности для $h = g \circ (x, y)$, $g, h \in S(V_n)$ примерно в 2^n раз быстрее по сравнению с алгоритмом его вычисления для произвольной подстановки. Трудоёмкость алгоритма вычисления линейности ℓ_h из работы [13] примерно в n раз меньше трудоёмкости её нахождения для произвольной подстановки.

Наиболее затратным этапом алгоритма 1 является вычисление ℓ_F, δ_F, линейного и разностного спектров. С целью оптимизации этих вычислений применим теорию из [13] для определения ячеек в DDT и LAT, в которых возникают изменения значений при умножении на транспозицию только 4-битовой подстановки $\widehat{\pi}_1$ или $\widehat{\pi}_2$ в обобщённой конструкции (1).

Утверждение 1. Пусть 8-битовая подстановка $G(z) = G(x_1, x_2) = y_1 \| y_2$, $z = x_1 \| x_2$, построена по формулам (1) с использованием одного из 768 наборов параметров $(\alpha, \beta, \gamma, \delta)$ [12] и произвольных 4-битовых подстановок $\widehat{\pi}_1$, $\widehat{\pi}_2$ (2), а подстановка H получена из G одной транспозицией подстановки $\widehat{\pi}_2$, т. е.

$$H = G \circ (0 \| x,\ 0 \| y), \quad x, y \in V_4^{\times}, \quad x \neq y. \tag{6}$$

Пусть $a \in V_8^{\times}$, $b \in V_8$ — произвольные, при этом $a = a_1 \| a_2$, $b = b_1 \| b_2$, $a_i, b_i \in V_4$, $i = 1, 2$. Тогда выполняются соотношения

$$\delta_H(a, b) - \delta_G(a, b) = \begin{cases} 0, & a_1 = 0,\ b_1 \neq 0, \\ 0, & a_1 = 0,\ b_1 = 0,\ a_2 = x + y, \\ 2(I_1 + I_3 - I_0 - I_2), & a_1 = 0,\ b_1 = 0,\ a_2 \neq x + y, \\ 2(\widetilde{I}_1 + \widetilde{I}_3 - \widetilde{I}_0 - \widetilde{I}_2), & a_1 \neq 0, \end{cases}$$

где

$$\begin{aligned} I_1 &= I_{b_2}(\widehat{\pi}_2(x+a_2)+\widehat{\pi}_2(y)), & I_3 &= I_{b_2}(\widehat{\pi}_2(y+a_2)+\widehat{\pi}_2(x)),\\ I_0 &= I_{b_2}(\widehat{\pi}_2(x+a_2)+\widehat{\pi}_2(x)), & I_2 &= I_{b_2}(\widehat{\pi}_2(y+a_2)+\widehat{\pi}_2(y)),\\ \widetilde{I}_1 &= I_b(g_{1,x}\|(g_{2,x}+\widehat{\pi}_2(y))), & \widetilde{I}_3 &= I_b(g_{1,y}\|(g_{2,y}+\widehat{\pi}_2(x))),\\ \widetilde{I}_0 &= I_b(g_{1,x}\|(g_{2,x}+\widehat{\pi}_2(x))), & \widetilde{I}_2 &= I_b(g_{1,y}\|(g_{2,y}+\widehat{\pi}_2(y))),\\ (g_{1,x}\|g_{2,x}) &= G(a_1,x+a_2), & (g_{1,y}\|g_{2,y}) &= G(a_1,y+a_2). \end{aligned} \tag{7}$$

Доказательство. По условию для 8-битовых подстановок H и G имеем

$$\begin{gathered} G(x_1,x_2)=H(x_1,x_2)\quad \forall x_1,x_2\,\big((x_1\neq 0)\text{ или }(x_1=0,\,x_2\neq x,\,x_2\neq y)\big),\\ G(0,x)=0\|\widehat{\pi}_2(x)=H(0,y),\quad G(0,y)=0\|\widehat{\pi}_2(y)=H(0,x). \end{gathered} \tag{8}$$

Далее, в силу определения 6 выпишем следующую цепочку соотношений:

$$\begin{gathered} \delta_H(a,b)-\delta_G(a,b)=\\ =|\{z\in V_8: H(z+a)+H(z)=b\}|-|\{z\in V_8\,|\,G(z+a)+G(z)=b\}|=\\ =\sum_{z\in V_8} I_b(H(z+a)+H(z))-\sum_{z\in V_8} I_b(G(z+a)+G(z))=\\ =2\sum_{z\in\{(0\|x),\,(0\|y)\}}(I_b(H(z+a)+H(z))-I_b(G(z+a)+G(z))). \end{gathered} \tag{9}$$

I. Пусть $a_1=0$, т. е. $a=0\|a_2$. При $b=b_1\|b_2$ и $b_1\neq 0$ из (9) с учётом вида функции (1) имеем $\delta_H(a,b)-\delta_G(a,b)=0$. Рассмотрим теперь случай $b=0\|b_2$.

I.1. Пусть $a_2=x+y$. В этом случае из равенств (9) непосредственно следует, что $\delta_H(a,b)-\delta_G(a,b)=0$, поскольку в силу (8) имеем $G(0,y)+G(0,x)=H(0,x)+H(0,y)$.

I.2. Пусть $a_2\neq x+y$, тогда соотношения (9) преобразуются к виду

$$\begin{gathered} \delta_H(a,b)-\delta_G(a,b)=2\big(I_{b_2}(\widehat{\pi}_2(x+a_2)+\widehat{\pi}_2(y))+I_{b_2}(\widehat{\pi}_2(y+a_2)+\widehat{\pi}_2(x))-\\ -I_{b_2}(\widehat{\pi}_2(x+a_2)+\widehat{\pi}_2(x))-I_{b_2}(\widehat{\pi}_2(y+a_2)+\widehat{\pi}_2(y))\big)=2(I_1+I_3-I_0-I_2). \end{gathered}$$

II. Пусть $a=a_1\|a_2$ и $a_1\neq 0$. В этом случае справедливы соотношения

$$\begin{aligned} G(a_1,x+a_2)+G(0,x)&=(g_{1,x}\|g_{2,x})+(0\|\widehat{\pi}_2(x))=g_{1,x}\|(g_{2,x}+\widehat{\pi}_2(x)),\\ G(a_1,y+a_2)+G(0,y)&=(g_{1,y}\|g_{2,y})+(0\|\widehat{\pi}_2(y))=g_{1,y}\|(g_{2,y}+\widehat{\pi}_2(y)),\\ H(a_1,x+a_2)+H(0,x)&=(g_{1,x}\|g_{2,x})+(0\|\widehat{\pi}_2(y))=g_{1,x}\|(g_{2,x}+\widehat{\pi}_2(y)),\\ H(a_1,y+a_2)+H(0,y)&=(g_{1,y}\|g_{2,y})+(0\|\widehat{\pi}_2(x))=g_{1,y}\|(g_{2,y}+\widehat{\pi}_2(x)). \end{aligned}$$

Тогда

$$\begin{gathered} \delta_H(a,b)-\delta_G(a,b)=2\Big[I_b(g_{1,x}\|(g_{2,x}+\widehat{\pi}_2(y)))+I_b(g_{1,y}\|(g_{2,y}+\widehat{\pi}_2(x)))-\\ -I_b(g_{1,x}\|(g_{2,x}+\widehat{\pi}_2(x)))-I_b(g_{1,y}\|(g_{2,y}+\widehat{\pi}_2(y)))\Big]=2(\widetilde{I}_1+\widetilde{I}_3-\widetilde{I}_0-\widetilde{I}_2). \end{gathered}$$

Утверждение 1 доказано. ■

Аналогично доказывается соответствующее утверждение относительно транспозиции подстановки $\widehat{\pi}_1$:

Утверждение 2. Пусть 8-битовая подстановка $G = G(x_1, x_2) = y_1 \| y_2$ построена по формулам (1) с использованием одного из 768 наборов параметров $(\alpha, \beta, \gamma, \delta)$ [12] и произвольных 4-битовых подстановок $\widehat{\pi}_1$, $\widehat{\pi}_2$ (2), а подстановка H получена из G одной транспозицией подстановки $\widehat{\pi}_1$, т. е.

$$H = G \circ (x\|0,\, y\|0), \quad x, y \in V_4^{\times}, \quad x \neq y.$$

Пусть $a \in V_8^{\times}$, $b \in V_8$ — произвольные, при этом $a = a_1\|a_2, b = b_1\|b_2$, тогда выполняются соотношения

$$\delta_H(a,b) - \delta_G(a,b) = \begin{cases} 0, & a_2 = 0,\ b_2 \neq 0, \\ 0, & a_2 = 0,\ b_2 = 0,\ a_1 = x + y, \\ 2(J_1 + J_3 - J_0 - J_2), & a_2 = 0,\ b_2 = 0,\ a_1 \neq x + y, \\ 2(\widetilde{J}_1 + \widetilde{J}_3 - \widetilde{J}_0 - \widetilde{J}_2), & a_2 \neq 0, \end{cases}$$

где

$$\begin{aligned} J_1 &= I_{b_1}(\widehat{\pi}_1(x + a_1) + \widehat{\pi}_1(y)), & J_3 &= I_{b_1}(\widehat{\pi}_1(y + a_1) + \widehat{\pi}_1(x)), \\ J_0 &= I_{b_1}(\widehat{\pi}_1(x + a_1) + \widehat{\pi}_1(x)), & J_2 &= I_{b_1}(\widehat{\pi}_1(y + a_1) + \widehat{\pi}_1(y)), \\ \widetilde{J}_1 &= I_b((\widetilde{g}_{1,x} + \widehat{\pi}_1(y))\|\widetilde{g}_{2,x}), & \widetilde{J}_3 &= I_b((\widetilde{g}_{1,y} + \widehat{\pi}_1(x))\|\widetilde{g}_{2,y}), \\ \widetilde{J}_0 &= I_b((\widetilde{g}_{1,x} + \widehat{\pi}_1(x))\|\widetilde{g}_{2,x}), & \widetilde{J}_2 &= I_b((\widetilde{g}_{1,y} + \widehat{\pi}_1(y))\|\widetilde{g}_{2,y}), \\ (\widetilde{g}_{1,x}\|\widetilde{g}_{2,x}) &= G(x + a_1, a_2), & (\widetilde{g}_{1,y}\|\widetilde{g}_{2,y}) &= G(y + a_1, a_2). \end{aligned} \tag{10}$$

Принимая во внимание определение 6 и утверждения 1 и 2, приходим к справедливости следующего следствия:

Следствие 1. Для подстановок H и G, рассматриваемых в утверждениях 1 и 2, выполняются неравенства (4).

Утверждения 1 и 2 позволяют, с учётом особенности обобщённой конструкции, конкретизировать индексы ячеек таблицы DDT, в которых появляются изменения при одной транспозиции во вспомогательной 4-битовой подстановке ($\widehat{\pi}_1$ или $\widehat{\pi}_2$). Так, можно указать множество ячеек DDT, значения в которых никогда не меняются при последовательном умножении на любые транспозиции только подстановки $\widehat{\pi}_1$ (или только подстановки $\widehat{\pi}_2$). Например, при последовательном умножении $\widehat{\pi}_2$ на транспозиции неизменными остаются ячейки DDT с индексами из прямоугольного диапазона $\{(a_1\|a_2, b_1\|b_2) : a_1 = 0, b_1 \neq 0\}$. Тем самым эту часть DDT можно не хранить в памяти. Утверждения 1 и 2 можно использовать в алгоритме пересчёта разностного спектра для новой подстановки, предложенном в работе [13, Algorithm 2, p. 117], при этом в силу формул (7), (10) операции побитового XOR будут осуществляться для 4-битовых векторов, а не для 8-битовых (см. далее алгоритм 2 для $\widehat{\pi}_2$). Отметим, что утверждения 1 и 2 могут быть сформулированы и доказаны аналогичным образом для обобщённой конструкции (1) при произвольном m. При этом асимптотическая оценка трудоёмкости нахождения дифференциальной δ-равномерности совпадет с приведённой в [13].

Алгоритм 2. Модификация [13, Algorithm 2, p. 117] при умножении на транспозицию подстановки $\widehat{\pi}_2$

Вход: 8-битовая подстановка $G = G(x_1, x_2) = y_1 \| y_2$, построенная по формулам (1) с использованием одного из 768 наборов параметров $(\alpha, \beta, \gamma, \delta)$ [12] и произвольных 4-битовых подстановок $\widehat{\pi}_1$, $\widehat{\pi}_2$ (2); $x, y \in V_4^{\times}$, $x \neq y$; DDT_G; разностный спектр D_G.

Для всех элементов $a_2 = 1, \ldots, 2^4 - 1$, таких, что $a_2 \neq x + y$:
  вычислить элементы $B_0 = \widehat{\pi}_2(x) + \widehat{\pi}_2(x + a_2)$ и $B_2 = \widehat{\pi}_2(y) + \widehat{\pi}_2(y + a_2)$.
  Если $B_0 = B_2$, **то**
    вычислить элемент $B_1 = \widehat{\pi}_2(y) + \widehat{\pi}_2(x + a_2)$.
    Для $i = 0, 1$ изменить значения:
      $\big|D_G(\delta_G(0\|a_2, 0\|B_i))\big| := \big|D_G(\delta_G(0\|a_2, 0\|B_i))\big| - 1$;
      $\delta_G(0\|a_2, 0\|B_i) := \delta_G(0\|a_2, 0\|B_i) + 4(-1)^{i+1}$;
      $\big|D_G\big(\delta_G(0\|a_2, 0\|B_i)\big)\big| := \big|D_G\big(\delta_G(0\|a_2, 0\|B_i)\big)\big| + 1$;
  иначе
    вычислить элементы $B_1 = \widehat{\pi}_2(y) + \widehat{\pi}_2(x + a_2)$ и $B_3 = \widehat{\pi}_2(x) + \widehat{\pi}_2(y + a_2)$.
    Для всех $i = 0, \ldots, 3$ изменить значения:
      $\big|D_G(\delta_G(0\|a_2, 0\|B_i))\big| := \big|D_G(\delta_G(0\|a_2, 0\|B_i))\big| - 1$;
      $\delta_G(0\|a_2, 0\|B_i) := \delta_G(0\|a_2, 0\|B_i) + 2(-1)^{i+1}$;
      $\big|D_G\big(\delta_G(0\|a_2, 0\|B_i)\big)\big| := \big|D_G\big(\delta_G(0\|a_2, 0\|B_i)\big)\big| + 1$.
Для всех элементов $a_1 \in V_4^{\times}$, $a_2 \in V_4$:
  вычислить $G(a_1, x + a_2) = (g_{1,x} \| g_{2,x})$, $G(a_1, y + a_2) = (g_{1,y} \| g_{2,y})$;
  вычислить элементы $B_0 = g_{1,x} \| (g_{2,x} + \widehat{\pi}_2(x))$ и $B_2 = g_{1,y} \| (g_{2,y} + \widehat{\pi}_2(y))$.
  Если $B_0 = B_2$, **то**
    вычислить элемент $B_1 = g_{1,x} \| (g_{2,x} + \widehat{\pi}_2(y))$.
    Для $i = 0, 1$ изменить значения:
      $\big|D_G(\delta_G(a_1\|a_2, B_i))\big| := \big|D_G(\delta_G(a_1\|a_2, B_i))\big| - 1$;
      $\delta_G(a_1\|a_2, B_i) := \delta_G(a_1\|a_2, B_i) + 4(-1)^{i+1}$;
      $\big|D_G\big(\delta_G(a_1\|a_2, B_i)\big)\big| := \big|D_G\big(\delta_G(a_1\|a_2, B_i)\big)\big| + 1$;
  иначе
    вычислить элементы $B_1 = g_{1,x} \| (g_{2,x} + \widehat{\pi}_2(y))$ и $B_3 = g_{1,y} \| (g_{2,y} + \widehat{\pi}_2(x))$.
    Для всех $i = 0, \ldots, 3$ изменить значения:
      $\big|D_G(\delta_G(a_1\|a_2, B_i))\big| := \big|D_G(\delta_G(a_1\|a_2, B_i))\big| - 1$;
      $\delta_G(a_1\|a_2, B_i) := \delta_G(a_1\|a_2, B_i) + 2(-1)^{i+1}$;
      $\big|D_G\big(\delta_G(a_1\|a_2, B_i)\big)\big| := \big|D_G\big(\delta_G(a_1\|a_2, B_i)\big)\big| + 1$.
Алгоритм останавливается после вычисления $H = G \circ (0\|x, 0\|y)$ и $D_H = D_G$.

Выход: Подстановка $H = G \circ (0\|x, 0\|y)$; DDT_H; разностный спектр D_H.

Теперь, учитывая особенности обобщённой конструкции (1) и тот факт, что на транспозицию умножается только одна из 4-битовых подстановок ($\widehat{\pi}_1$ или $\widehat{\pi}_2$), найдём индексы ячеек LAT, в которых происходят изменения в результате умножения на транспозицию. Приведём два прямых следствия из соответствующего предложения [13].

Утверждение 3. Пусть 8-битовая подстановка $G = G(x_1, x_2) = y_1 \| y_2$ построена по формулам (1) с использованием одного из 768 наборов параметров $(\alpha, \beta, \gamma, \delta)$ [12] и произвольных 4-битовых подстановок $\widehat{\pi}_1$, $\widehat{\pi}_2$ (2), а подстановка H получена из G одной транспозицией подстановки $\widehat{\pi}_2$, т. е.

$$H = G \circ (0\|x,\ 0\|y), \quad x, y \in V_4^{\times}, \quad x \neq y.$$

Пусть $a \in V_8$, $b \in V_8^\times$ — произвольные, при этом $a = a_1 \| a_2, b = b_1 \| b_2$, тогда выполняются соотношения

$$\ell_H(a,b) - \ell_G(a,b) = \begin{cases} 0, & \langle a_2,\, x+y\rangle = 0 \text{ или } \langle b_2, \widehat{\pi}_2(x) + \widehat{\pi}_2(y)\rangle = 0, \\ (-1)^{\langle a_2,\, x\rangle + \langle b_2, \widehat{\pi}_2(x)\rangle + 1} \cdot 2 & \text{в противном случае.} \end{cases} \tag{11}$$

Утверждение 4. Пусть 8-битовая подстановка $G = G(x_1, x_2) = y_1 \| y_2$ построена по формулам (1) с использованием одного из 768 наборов параметров $(\alpha, \beta, \gamma, \delta)$ [12] и произвольных 4-битовых подстановок $\widehat{\pi}_1$, $\widehat{\pi}_2$ (2), а подстановка H получена из G одной транспозицией подстановки $\widehat{\pi}_1$, т. е.

$$H = G \circ (x\|0,\, y\|0), \quad x, y \in V_4^\times, \quad x \neq y.$$

Пусть $a \in V_8$, $b \in V_8^\times$ — произвольные, при этом $a = a_1 \| a_2, b = b_1 \| b_2$, тогда выполняются соотношения

$$\ell_H(a,b) - \ell_G(a,b) = \begin{cases} 0, & \langle a_1,\, x+y\rangle = 0 \text{ или } \langle b_1, \widehat{\pi}_1(x) + \widehat{\pi}_1(y)\rangle = 0, \\ (-1)^{\langle a_1,\, x\rangle + \langle b_1, \widehat{\pi}_1(x)\rangle + 1} \cdot 2 & \text{в противном случае.} \end{cases} \tag{12}$$

Следствие 2. В условиях утверждений (3) и (4) значения в следующих ячейках LAT исходной 8-битовой подстановки не изменяются при последовательном умножении в произвольном порядке вспомогательных 4-битовых подстановок $\widehat{\pi}_1$, $\widehat{\pi}_2$ на транспозиции (x, y), $x, y \in V_4^\times$, $x \neq y$:

$$\{(a_1\|a_2, b_1\|b_2) : a_1 = b_2 = 0, \text{ или } a_2 = b_1 = 0, \text{ или } a_1 = a_2 = 0, \text{ или } b_1 = b_2 = 0\}. \tag{13}$$

Доказательство. В силу утверждения 3 при умножении $\widehat{\pi}_2$ на транспозицию не изменяются значения LAT в ячейках с индексами $\{(a_1\|a_2, b_1\|b_2) : a_2 = 0 \text{ или } b_2 = 0\}$. В силу утверждения 4 при умножении $\widehat{\pi}_1$ на транспозицию не изменяются значения LAT в ячейках с индексами $\{(a_1\|a_2, b_1\|b_2) : a_1 = 0 \text{ или } b_1 = 0\}$. В пересечении этих множеств получим указанное в следствии множество индексов. ■

В свою очередь, из определений 10 и 11 и утверждений 3 и 4 непосредственно вытекает

Следствие 3. Для подстановок H и G, рассматриваемых в утверждениях 3 и 4, выполняются неравенства (5).

Утверждения 3 и 4 и следствие 2 можно использовать в алгоритме пересчёта линейного спектра, предложенном в [13, Algorithm 1, p. 114], применяя его к подстановкам, полученным путём умножения на транспозицию вспомогательных подстановок $\widehat{\pi}_1$ или $\widehat{\pi}_2$ в обобщённой конструкции (1). При этом значения ячеек LAT с индексами (13) можно не хранить в памяти, а также в силу формул (11) и (12) операции скалярного произведения выполнять для 4-битовых векторов, а не для 8-битовых (алгоритм 3 для $\widehat{\pi}_2$). Отметим, что утверждения 3 и 4 справедливы для обобщённой конструкции (1) при произвольном m. При этом асимптотическая оценка трудоёмкости нахождения линейности совпадет с приведённой в [13].

Алгоритм 3. Модификация [13, Algorithm 1, p. 114] при умножении на транспозицию подстановки $\widehat{\pi}_2$

Вход: 8-битовая подстановка $G = G(x_1, x_2) = y_1 \| y_2$, построенная по формулам (1) с использованием одного из 768 наборов параметров $(\alpha, \beta, \gamma, \delta)$ [12] и произвольных 4-битовых подстановок $\widehat{\pi}_1$, $\widehat{\pi}_2$ (2); $x, y \in V_4^{\times}$, $x \neq y$; LAT_G; линейный спектр L_G.

1: Вычислить элементы $a_2 = x + y$ и $b_2 = \widehat{\pi}_2(x) + \widehat{\pi}_2(y)$.
2: **Для всех** элементов $i = 1, \ldots, 2^4 - 1$ выполнить:
3: **Если** $\langle a_2, i\rangle > 0$, **то**
4: добавить i в список I_1.
5: **Если** $\langle b_2, i\rangle > 0$, **то**
6: добавить i в список I_2.
7: **Для всех** пар $(a_2, b_2) \in I_1 \times I_2$ выполнить:
8: вычислить $\Delta\ell(a_2, b_2) = (-1)^{\langle a_2, x\rangle + \langle b_2, \widehat{\pi}_2(x)\rangle + 1} \cdot 2$.
9: **Для всех** $a_1 \in V_4$, $b_1 \in V_4$
10: сформировать $a = a_1 || a_2$, $b = b_1 || b_2$;
11: вычислить $|L_G(|\ell_G(a, b)|)| := |L_G(|\ell_G(a, b)|)| - 1$;
12: вычислить значение $\ell_G(a, b) := \ell_G(a, b) + \Delta\ell(a_2, b_2)$;
13: вычислить $|L_G(|\ell_G(a, b)|)| := |L_G(|\ell_G(a, b)|)| + 1$.
14: Алгоритм останавливается после вычисления $H = G \circ (0\|x, 0\|y)$ и $L_H = L_G$.

Выход: Подстановка $H = G \circ (0\|x, 0\|y)$; LAT_H; линейный спектр L_H.

Заключение

Предложен эвристический алгоритм подбора таких вспомогательных 4-битовых подстановок в обобщённой конструкции, полученных посредством умножения на транспозиции, чтобы итоговая 8-битовая подстановка F обладала криптографическими характеристиками $N_F = 108$, $\delta_F = 6$. Экспериментально показана практическая применимость алгоритма, при этом удалось получить подстановки с минимальной степенью 7. Теоретически исследованы вопросы оптимизации вычисления линейного и разностного спектров на каждой итерации алгоритма. Алгоритмы вычисления линейного и разностного спектров из работы [13] применены к подстановкам, задаваемым конструкцией (1), с учётом того, что на транспозицию умножается одна из вспомогательных 4-битовых подстановок. При реализации алгоритмов можно получить выигрыш по памяти за счёт уменьшения числа хранимых ячеек в DDT и LAT. При этом операции побитового XOR и вычисления скалярного произведения осуществляются для 4-битовых векторов, а не для 8-битовых.

ЛИТЕРАТУРА

1. *Biham E. and Shamir A.* Differential cryptanalysis of the full 16-round DES // LNCS. 1993. V. 740. P. 487–496.
2. *Biham E. and Shamir A.* Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. No. 4. P. 3–72.
3. *Matsui M.* Linear cryptanalysis method for DES cipher // LNCS. 1994. V. 765. P. 386–397.
4. *Shannon C. E.* Communication theory of secrecy systems // Bell Syst. Techn. J. 1949. V. 28. P. 656–715.
5. *Menyachikhin A. V.* Spectral-linear and spectral-differential methods for generating S-boxes having almost optimal cryptographic parameters // Матем. вопр. криптогр. 2017. Т. 8. № 2. С. 97–116.

6. *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 // LNCS. 2019. V. 11368. P. 191–206.
7. *De la Cruz Jiménez R.A.* On Some Methods for Constructing Almost Optimal S-Boxes and their Resilience against Side-Channel Attacks. 2018. `https://eprint.iacr.org/2018/618`.
8. *De la Cruz Jiménez R.A.* A method for constructing permutations, involutions and orthomorphisms with strong cryptographic properties // Прикладная дискретная математика. Приложение. 2019. № 12. С. 145–151.
9. *Фомин Д. Б.* О подходах к построению низкоресурсных нелинейных преобразований // Обозрение прикладной и промышленной математики. 2018. Т. 25. Вып. 4. С. 379–381.
10. *Fomin D. B.* New classes of 8-bit permutations based on a butterfly structure // Матем. вопр. криптогр. 2019. Т. 10. № 2. С. 169–180.
11. *Фомин Д. Б.* Построение подстановок пространства V_{2m} с использованием $(2m, m)$-функций // Матем. вопр. криптогр. 2020. Т. 11. № 3. С. 121–138.
12. *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.
13. *Menyachikhin A.* The change in linear and differential characteristics of substitution after the multiplication by transposition // Матем. вопр. криптогр. 2020. Т. 11. № 2. С. 111–123.
14. *Fomin D. and Kovrizhnykh M.* On differential uniformity of permutations derived using a generalized construction // CTCrypt 2021. `https://ctcrypt.ru/files/files/2021/Fomin_Kovrizhnylh.pdf`.
15. *Ivanov G., Nikolov N., and Nikova S.* Reversed genetic algorithms for generation of bijective s-boxes with good cryptographic properties // Cryptogr. Commun. 2016. V. 8. No. 2. P. 247–276.
16. *Biryukov A., Perrin L., and Udovenko A.* Reverse-engineering the s-box of Streebog, Kuznyechik and STRIBOBr1 // LNCS. 2016. V. 9665. P. 372–402.
17. *Canteaut A. and Perrin L.* On CCZ-Equivalence, Extended-Affine Equivalence, and Function Twisting. Cryptology ePrint Archive, Report 2018/713. `https://eprint.iacr.org/2018/713`.
18. *Kazymyrov O. V., Kazymyrova V. N., and Oliynykov R. V.* A method for generation of high-nonlinear S-boxes based on gradient descent // Матем. вопр. криптогр. 2014. Т. 5. № 2. С. 71–78.
19. *Лидл Р., Нидеррайтер Г.* Конечные поля. В 2-х т. М.: Мир, 1988. 430 с.
20. *Кострикин А. И.* Введение в алгебру. Ч. I. Основы алгебры: учебник для вузов. 3-е изд. М.: Физматлит, 2004. 272 с.
21. *Browning K. A., Dillon J. F., McQuistan M. T., and Wolfe A. J.* An APN permutation in dimension six // 9th Int. Conf. Finite Fields Appl. 2009. Contemp. Math. 2010. V. 518. P. 33–42.
22. *Knuth D.* Art of Computer Programming. V. 2: Seminumerical Algorithms, 3rd ed. Addison-Wesley Professional, 1997.
23. *Казимиров А. В.* Методы и средства генерации нелинейных узлов замены для симметричных криптоалгоритмов: дис. ... канд. техн. наук. Харьков, 2013. 190 с.
24. *O'Connor L.* Properties of linear approximation tables // LNCS. 1995. V. 1008. P. 131–136.
25. *Carlet C.* Vectorial Boolean functions for cryptography // Boolean Models and Methods in Mathematics, Computer Science, and Engineering / eds. Y. Crama and P. Hammer. Cambridge: Cambridge University Press, 2010. P. 398–469.

26. *Yu Y., Wang M., and Li Y.* Constructing differential 4-uniform permutations from know ones. Cryptology ePrint Archive. Report 2011/047. 2011. https://eprint.iacr.org/2011/047.

REFERENCES

1. *Biham E. and Shamir A.* Differential cryptanalysis of the full 16-round DES. LNCS, 1993, vol. 740, pp. 487–496.
2. *Biham E. and Shamir A.* Differential cryptanalysis of DES-like cryptosystems. J. Cryptology, 1991, no. 4, pp. 3–72.
3. *Matsui M.* Linear cryptanalysis method for DES cipher. LNCS, 1994, vol. 765, pp. 386–397.
4. *Shannon C. E.* Communication theory of secrecy systems. Bell Syst. Techn. J., 1949, vol. 28, pp. 656–715.
5. *Menyachikhin A. V.* Spectral-linear and spectral-differential methods for generating S-boxes having almost optimal cryptographic parameters. Mat. Vopr. Kriptogr., 2017, vol. 8, iss. 2, pp. 97–116.
6. *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. LNCS, 2019, vol. 11368, pp. 191–206.
7. *De la Cruz Jiménez R.A.* On Some Methods for Constructing Almost Optimal S-Boxes and their Resilience against Side-Channel Attacks. 2018. https://eprint.iacr.org/2018/618.
8. *De la Cruz Jiménez R.A.* A method for constructing permutations, involutions and orthomorphisms with strong cryptographic properties. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2019, no. 12, pp. 145–151.
9. *Fomin D. B.* O podkhodakh k postroeniyu nizkoresursnykh nelineynykh preobrazovaniy [On approaches to constructing low-resource nonlinear transformations]. Obozrenie Prikladnoy i Promyshlennoy Matematiki, 2018, vol. 25, iss. 4, pp. 379–381. (in Russian)
10. *Fomin D. B.* New classes of 8-bit permutations based on a butterfly structure. Mat. Vopr. Kriptogr., 2019, vol. 10, no. 2, pp. 169–180.
11. *Fomin D. B.* Postroenie podstanovok prostranstva V_{2m} s ispol'zovaniem $(2m, m)$-funktsiy [Construction of permutations on the space V_{2m} by means of $(2m, m)$-functions]. Mat. Vopr. Kriptogr., 2020, vol. 11, no. 3, pp. 121–138. (in Russian)
12. *Fomin D. B.* Ob algebraicheskoy stepeni i differentsial'noy ravnomernosti podstanovok prostranstva V_{2m}, postroyennykh s ispol'zovaniyem $(2m, m)$-funktsiy [On the algebraic degree and differential uniformity of permutations on the space V_{2m} constructed via $(2m, m)$-functions]. Mat. Vopr. Kriptogr., 2020, vol. 11, no. 4. pp. 133–149. (in Russian)
13. *Menyachikhin A.* The change in linear and differential characteristics of substitution after the multiplication by transposition. Mat. Vopr. Kriptogr., 2020, vol. 11, no. 2, pp. 111–123.
14. *Fomin D. and Kovrizhnykh M.* On differential uniformity of permutations derived using a generalized construction. CTCrypt 2021. https://ctcrypt.ru/files/files/2021/Fomin_Kovrizhnylh.pdf.
15. *Ivanov G., Nikolov N., and Nikova S.* Reversed genetic algorithms for generation of bijective s-boxes with good cryptographic properties. Cryptogr. Commun., 2016, vol. 8, no. 2, pp. 247–276.
16. *Biryukov A., Perrin L., and Udovenko A.* Reverse-engineering the s-box of Streebog, Kuznyechik and STRIBOBr1. LNCS, 2016, vol. 9665, pp. 372–402.
17. *Canteaut A. and Perrin L.* On CCZ-Equivalence, Extended-Affine Equivalence, and Function Twisting. Cryptology ePrint Archive, Report 2018/713. https://eprint.iacr.org/2018/713.

18. *Kazymyrov O. V., Kazymyrova V. N., and Oliynykov R. V.* A method for generation of high-nonlinear S-boxes based on gradient descent. Mat. Vopr. Kriptogr., 2014, vol. 5, no. 2, pp. 71–78.
19. *Lidl R. and Niederreiter H.* Finite Fields. 2nd ed. Cambridge, Cambridge University Press, 1997. 755 p.
20. *Kostrikin A. I.* Introduction to Algebra. N.Y., Springer Verlag, 1982. 577 p.
21. *Browning K. A., Dillon J. F., McQuistan M. T., and Wolfe A. J.* An APN permutation in dimension six. 9th Int. Conf. Finite Fields Appl. 2009; Contemp. Math., 2010, vol. 518, pp. 33–42.
22. *Knuth D.* Art of Computer Programming. Vol. 2: Seminumerical Algorithms, 3rd ed. Addison-Wesley Professional, 1997.
23. *Kazymyrov O. V.* Metody i sredstva generatsii nelineynykh uzlov zameny dlya simmetrichnykh kriptoalgoritmov [Methods and tools for generating nonlinear replacement nodes for symmetric cryptographic algorithms]. PhD Thesis, Kharkiv, 2013. 190 p. (in Russian)
24. *O'Connor L.* Properties of linear approximation tables. LNCS, 1995. vol. 1008, pp. 131–136.
25. *Carlet C.* Vectorial Boolean functions for cryptography. Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Y. Crama and P. Hammer (eds.). Cambridge: Cambridge University Press, 2010, pp. 398–469.
26. *Yu Y., Wang M., and Li Y.* Constructing differential 4-uniform permutations from know ones. Cryptology ePrint Archive, Report 2011/047, 2011. `https://eprint.iacr.org/2011/047`.