Секция 7

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

УДК 519.719.2 DOI 10.17223/2226308X/14/42

ОБ ЭВРИСТИЧЕСКОМ ПОДХОДЕ К ПОСТРОЕНИЮ БИЕКТИВНЫХ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ С ЗАДАННЫМИ КРИПТОГРАФИЧЕСКИМИ ХАРАКТЕРИСТИКАМИ

М. А. Коврижных, Д. Б. Фомин

Предложен эвристический алгоритм построения биективных булевых функций с заданными криптографическими свойствами — нелинейностью и дифференциальной δ-равномерностью — на основе обобщённой конструкции. Производится поиск вспомогательных подстановок меньшей размерности в обобщённой конструкции с использованием идей спектрально-линейного и спектрально-разностного методов. Исследована возможность оптимизации вычисления криптографических характеристик на каждой итерации алгоритма. Экспериментально получены 8-битовые 6-равномерные подстановки с нелинейностью 108.

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

Биективные векторные булевы функции (подстановки) используются в качестве нелинейных примитивов многих симметричных шифров. Построение подстановок размерности $n \geqslant 8$ бит с криптографическими характеристиками, гарантирующими стойкость шифров к разностному и линейному методам криптоанализа, является сложной задачей.

В [1] представлены спектрально-линейный и спектрально-разностный методы генерации подстановок, основанные на итеративном улучшении их криптографических характеристик путём умножения на транспозиции.

В [2, 3] описана обобщённая конструкция векторных булевых $(2m, 2m)$-функций, использующая мономиальные и произвольные подстановки размерности m. В случае $m = 4$ экспериментально найдены 768 наборов показателей степеней мономов, перспективных для построения 8-битовых 6-равномерных подстановок, имеющих нелинейность 108 и алгебраическую степень 7 при правильном выборе вспомогательных 4-битовых подстановок.

В настоящей работе предложен эвристический алгоритм поиска таких 4-битовых подстановок в обобщённой конструкции, при этом используются идеи спектрально-линейного и спектрально-разностного методов.

Обозначим: V_n — n-мерное векторное пространство над полем из двух элементов $\mathbb{F}_2$; $V_n^\times = V_n \setminus \{0\}$; $S(V_n)$ — симметрическую группу всех подстановок пространства V_n; $\mathbb{F}_{2^n}$ — конечное поле из 2^n элементов. Пусть $a \in V_n$, $b \in V_m$. *Конкатенацию* двух векторов будем обозначать как $a\|b \in V_{n+m}$. *Скалярным произведением* двух векторов $a, b \in V_n$ называется элемент поля $\mathbb{F}_2$, вычисляемый по формуле $\langle a, b\rangle = a_{n-1}b_{n-1} + {} + \ldots + a_0b_0$. *Транспозиция* — это цикл длины 2. Умножение подстановки G на транспо-

зицию справа $G \circ (i_1, i_2)$ приводит к транспозиции элементов i_1 и i_2 в верхней строке подстановки G [4, с. 51], другими словами, в нижней строке подстановки G меняются местами образы элементов i_1 и i_2.

Приведём определения некоторых криптографических характеристик подстановок.

Подстановка $F \in S(V_n)$ называется *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* подстановки F.

Таблицей распределения разностей (Difference Distribution Table — DDT) подстановки 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 $D_F(\delta) = \{(a, b) \in V_n^\times \times V_n : \delta_F(a, b) = \delta\}$. *Разностным спектром* подстановки F называется множество пар $D_F = \{(\delta, |D_F(\delta)|)\}$.

Преобразованием Уолша — Адамара $W_F(a, b)$ подстановки $F \in S(V_n)$ называется отображение $W_F : V_n \times V_n \to \mathbb{Z}$, заданное равенством

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

Линейность ℓ_F подстановки F определяется как $\ell_F = \max\limits_{a \in V_n,\, b \in V_n^\times} |W_F(a, b)|$. *Нелинейность* N_F подстановки F вычисляется по формуле $N_F = 2^{n-1} - \dfrac{1}{2}\ell_F$.

Таблицей линейных приближений (Linear Approximation Table — LAT) [5] подстановки 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 $L_F(\ell) = \{(a, b) \in V_n \times \times V_n^\times : \big|\ell_F(a, b)\big| = \ell\}$. *Линейным спектром* подстановки F называется множество пар $L_F = \{(\ell, |L_F(\ell)|)\}$.

Алгебраической степенью $\deg(F)$ подстановки F называется минимальная степень многочленов Жегалкина для всевозможных линейных комбинаций её координатных функций $\langle a, F(x) \rangle$ по всем $a \in V_n^\times$: $\deg(F) = \min\limits_{a \in V_n^\times} \deg(\langle a, F(x) \rangle)$.

Рассмотрим $(2m, 2m)$-функцию $F(x_1, x_2) = y_1 \| y_2$, где $x_1, x_2, y_1, y_2 \in V_m$, задаваемую следующей *обобщённой* конструкцией [2]:

$$y_1 = G_1(x_1, x_2) = \begin{cases} x_1^\alpha \cdot x_2^\beta, & x_2 \neq 0, \\ \widehat{\pi}_1(x_1), & x_2 = 0, \end{cases} \qquad y_2 = G_2(x_1, x_2) = \begin{cases} x_1^\gamma \cdot x_2^\delta, & x_1 \neq 0, \\ \widehat{\pi}_2(x_2), & x_1 = 0. \end{cases} \tag{1}$$

В силу существования взаимно-однозначного отображения $V_m \to \mathbb{F}_{2^m}$ в (1) и далее операции возведения в степень и умножения производятся в поле $\mathbb{F}_{2^m}$.

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

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

Отметим, что конструкция (1) основана на структуре типа «бабочка», предложенной в [6] и полученной при изучении декомпозиции APN-подстановки Диллона [7], и допускает TU-представление [8].

Далее исследуем обобщённую конструкцию (1) в случае $m = 4$ с одним из 768 наборов параметров $(\alpha, \beta, \gamma, \delta)$, приведённых в [3]. Поскольку подстановки $\widehat{\pi}_1$, $\widehat{\pi}_2$ в (1) выбираются независимо от параметров $(\alpha, \beta, \gamma, \delta)$, предложим эвристический алгоритм поиска таких 4-битовых подстановок $\widehat{\pi}_1$, $\widehat{\pi}_2$, чтобы итоговая 8-битовая подстановка (1) обладала заданными криптографическими характеристиками $N_F = 108$, $\delta_F = 6$. Вопрос о возможности получения с использованием конструкции (1) подстановок с $N_F > 108$, $\delta_F \leqslant 6$ требует дополнительного исследования.

Идея алгоритма 1 заключается в итеративном умножении начальных случайно сгенерированных 4-битовых подстановок на транспозиции и отбора среди полученных по формулам (1) 8-битовых подстановок, лучших по нелинейности, показателю дифференциальной равномерности и соответствующим значениям в линейном и разностном спектрах.

Алгоритм 1.

Вход: Подстановка $F \in S(V_8)$, построенная по формулам (1) с использованием одного из 768 наборов параметров $(\alpha, \beta, \gamma, \delta)$ [3] 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**
13: **Вывести** подстановки $\widehat{\pi}_1, \widehat{\pi}_2$, порождающие подстановку F,
14: **иначе**
15: Сформировать новый список $Best$ из Num_Best пар подстановок $(\widehat{\pi}_1, \widehat{\pi}_2)$, соответствующих лучшим наборам, отобранным на шаге 11.
16: **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 параметрами алгоритма. Вычислительные эксперименты показали, что при $Num\_Best = 10$, $Num\_Trans = 500$ на первой итерации и $Num\_Trans = 100$ на последующих за приемлемое число итераций можно получить 8-битовые подстановки с характеристиками (3) и алгебраической степенью 7.

Наиболее трудоёмким этапом алгоритма является вычисление ℓ_F, δ_F, линейного и разностного спектров. С целью оптимизации этих вычислений теория из работы [9] применена для определения ячеек в DDT и LAT, в которых возникают изменения значений при умножении на транспозицию только 4-битовой подстановки $\widehat{\pi}_1$ или $\widehat{\pi}_2$. Асимптотические оценки трудоёмкости нахождения разностного спектра, дифференциальной равномерности, линейного спектра и линейности совпадают с приведёнными в [9]. Так, алгоритм вычисления разностного спектра и показателя дифференциальной равномерности примерно в 2^{2m} раз быстрее по сравнению с алгоритмом их вычисления для произвольной подстановки, а трудоёмкость алгоритма пересчёта линейного спектра и линейности примерно в $2m$ раз меньше трудоёмкости их нахождения для произвольной подстановки. По сравнению с [9] при вычислении криптографических характеристик можно получить выигрыш по памяти за счёт уменьшения числа хранимых ячеек в DDT и LAT в силу особенностей обобщённой конструкции.

ЛИТЕРАТУРА

1. *Menyachikhin A. V.* Spectral-linear and spectral-differential methods for generating S-boxes having almost optimal cryptographic parameters // Матем. вопр. криптогр. 2017. Т. 8. Вып. 2. С. 97–116.
2. *Фомин Д. Б.* О подходах к построению низкоресурсных нелинейных преобразований // Обозрение прикладной и промышленной математики. 2018. Т. 25. Вып. 4. С. 379–381.
3. *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.
4. *Кострикин А. И.* Введение в алгебру. Ч. I. Основы алгебры: учебник для вузов. 3-е изд. М.: Физматлит, 2004. 272 с.
5. *O'Connor L.* Properties of linear approximation tables // LNCS. 1995. V. 1008. P. 131–136.
6. *Biryukov A., Perrin L., and Udovenko A.* Reverse-engineering the s-box of Streebog, Kuznyechik and STRIBOBr1 // LNCS. 2016. V. 9665. P. 372–402.
7. *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.
8. *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`.
9. *Menyachikhin A. V.* The change in linear and differential characteristics of substitution after the multiplication by transposition // Матем. вопр. криптогр. 2020. Т. 11. № 2. С. 111–123.

УДК 519.688 DOI 10.17223/2226308X/14/43

О НЕКОТОРЫХ ПОДГРУППАХ БЕРНСАЙДОВОЙ ГРУППЫ $B_0(2,5)$

А. А. Кузнецов, А. С. Кузнецова

Пусть $B_0(2,5) = \langle x, y\rangle$ — наибольшая конечная двупорождённая бернсайдова группа периода 5, порядок которой равен 5^{34}. В работе изучена серия подгрупп $H_i = \langle a_i, b_i\rangle$ группы $B_0(2,5)$, где $a_0 = x$, $b_0 = y$, $a_i = a_{i-1}b_{i-1}$ и $b_i = b_{i-1}a_{i-1}$