О КЛАССИФИКАЦИИ ПЛАТОВИДНЫХ УСТОЙЧИВЫХ БУЛЕВЫХ ФУНКЦИЙ, ПОРОЖДАЕМЫХ ОДНОЙ РЕКУРСИВНОЙ КОНСТРУКЦИЕЙ, ДЛЯ СЛУЧАЯ СОХРАНЕНИЯ МОЩНОСТИ НОСИТЕЛЯ СПЕКТРА

Е. В. Хинко (Москва)

Вопросы корреляционной иммунности и устойчивости булевых функций в настоящее время нередко поднимаются в работах многих авторов. Например, в [1, 2, 4] затрагивается проблема устойчивости функций при максимальных значениях нелинейности, в частности для случая $m > n/2 - 2$, где m – порядок устойчивости функции, а n – число переменных, оценка нелинейности булевой функции была усилена тремя группами авторов до $nl(f) < 2^{n-1} - 2^{m+1}$ при $m \leqslant n - 2$, при этом если граница достигается, то $m > 0.5 \cdot n - 2$.

Также было показано, что верхние оценки нелинейности достигаются на платовидных булевых функциях. *Платовидными* называют булевы функции, у которых множество значений коэффициентов Уолша принадлежит множеству $\{0, \pm 2^c\}$, где c (*амплитуда платовидности*) — натуральная константа, не зависящая от числа переменных n.

Представляет интерес построение и классификация конструкций, в частности рекурсивных, платовидных m-устойчивых булевых функций, позволяющих относительно легко получить функции от большого числа переменных с достаточно хорошим порядком устойчивости. В работах [1–3] затрагиваются вопросы устойчивости функций при максимальных значениях нелинейности и построены соответствующие рекурсивные конструкции m-устойчивых функций для $n - 2 \geqslant m \geqslant 0.6n - 1$.

Автор настоящей статьи проводит исследование конструкций с шагом числа переменных три. В общем виде задачу можно сформулировать следующим образом: пусть имеются b, $b \in \mathbb{N}$, платовидных m-устойчивых булевых функций от n переменных $f_n^i(x_1, x_2, \ldots, x_n)$, $i = \overline{1, b}$, среди которых, возможно, есть совпадающие с точностью до взятия отрицания; добавим три переменные x_{n+1}, x_{n+2} и x_{n+3}. Новые функции от $n + 3$ переменных обозначим $f_{n+3}^s(x_1, x_2, \ldots, x_n, x_{n+1}, x_{n+2}, x_{n+3})$, $s = \overline{1, 8}$.

Кратко это можно записать в виде вектор-строки:

$$\begin{pmatrix} f_{n+3}^s = & \sigma_{s1} g_{s1} & |\sigma_{s2} g_{s2} & |\sigma_{s3} g_{s3} & |\sigma_{s4} g_{s4}| \\ & |\sigma_{s5} g_{s5} & |\sigma_{s6} g_{s6} & |\sigma_{s7} g_{s7} & |\sigma_{s8} g_{s8} \end{pmatrix}, \qquad (1)$$

где $g_{sj} = f_n^i$ или $g_{sj} = \overline{f_n^i}$; $s, j = \overline{1,8}; i = \overline{1,b}$, а выбор функции или её отрицания зависит от значения индикатора σ_{sj}.

Представляет интерес подбор соотношений индикаторов σ_{sj} и порождающих функций f_n^i, чтобы для полученных новых функций от $n+3$ переменных выполнялись следующие свойства:

а) сохранение свойства платовидности;

б) обеспечение роста устойчивости;

в) рекурсивное воспроизведение конструкции.

Данная задача естественным образом распадается на два случая: случай увеличения мощности носителя спектра в 4 раза при применении конструкции и случай сохранения мощности носителя спектра при применении конструкции.

Для первого случая в [5, 6] автором была построены конструкции с примерами начальных функций для случая $b = 4$ различных функций, в [7] рассматривался вопрос несуществования рекурсивных конструкций с начальными условиями, для которых каждый двоичный набор содержится в носителях спектра ровно 6 и ровно 4 или 6 функций.

Также представляют интерес конструкции, сохраняющие мощность носителя спектра.

На данный момент автором рассмотрены случаи 1, 2, 3 и 4 различных порождающих функций. В случае трёх порождающих конструкций вида (1) не существует, а для 1, 2 и 4 различных порождающих верна следующая теорема:

Теорема. *Конструкция общего вида* (1) *сохраняет платовидность, мощность носителя спектра и обеспечивает рост устойчивости, если и только если:*

— случай одной порождающей функции f_n: $\sigma_{si} = \mathfrak{m}_{ki} \forall i = \overline{1,8}$, или $\sigma_{si} = -\mathfrak{m}_{ki} \forall i = \overline{1,8}$, где $\mathfrak{m}_{ki}$ — i-й элемент k-й строки матрицы Адамара-Сильвестра порядка 8;

— случай двух различных порождающих функций f_n^I и f_n^{II}: восемь порождающих функций $f_n^{i_j}, j = \overline{1,8}$, разбиваются на два подмножества по четыре функции (f_n^I и f_n^{II}), которые при этом удовлетворяют условиям ($u\alpha$) и ($u\beta$).

($u\alpha$) *Среди множества порождающих функций f_n^i, $i \in \overline{1,8}$, в каждой из половин $i = 1,2,3,4$ и $i = 5,6,7,8$ должно быть чётное число функций f_n^I и f_n^{II}.*

($u\beta$) *Если оба подмножества из четырёх порождающих функций f_n^I и f_n^{II} содержат по два представителя в каждой из половин $i = 1,2,3,4$, и $i = 5,6,7,8$, то в каждой из половин эти представи-*

тели должны располагаться на симметричных относительно центра строки или совпадающих местах с функциями другой половины.

— случай четырёх различных порождающих функций f_n^I, f_n^{II}, f_n^{III}, f_n^{IV} *:*
$\prod_{i=I}^{IV} W_{f_n^i} \geqslant 0$ *и порождающие функции* $f_n^{i_j}, j = \overline{1,8}$, *разбиваются на четыре подмножества по две (различные) функции, взаимное расположение пар которых удовлетворяет условиям* $(и\alpha)$ *и* $(и\beta)$.

Список литературы

1. Fedorova M., Tarannikov Yu. On the constructing of highly nonlinear resilient Boolean functions by means of special matrices // Progress in Cryptology – Indocrypt 2001, Chennai, India, December 16-20, 2001, Proceedings, Lecture Notes in Computer Science. — V. 2247. — P. 254–256.

2. Pasalic E., Maitra S., Johansson T., Sarkar P. New constructions of resilient and correlation immune Boolean functions achieving upper bounds of nonlinearity // WCC2001 International Workshop on Coding and Cryptography Electronic Notes in Discrete Mathematics. —2001. — V. 6.

3. Tarannikov Yu. New constructions of resilient boolean functions with maximal nonlinearity // Fast Software Encryption. 8th International Workshop, FSE 2001,Yokohama, Japan, April 2–4, 2001. Revised Papers, volume 2355 of Lecture notes in computer science. — P. 66–77.

4. Zheng Y., Zhang X. M. Improved upper bound on the nonlinearity of high order correlation immune functions // Selected Ares in Cryptography, 7th Annual International Workshop, SAC2000, Lecture Notes in Computer Science. — 2012. — P. 264–274.

5. Хинко Е. В. Об одной рекурсивной конструкции платовидных устойчивых булевых функций с шагом числа переменных 3 // ПДМ. — 2016. — № 1(31). — С. 92–103.

6. Хинко Е. В. О расширении возможностей конструкции платовидных m-устойчивых булевых функций // Интеллектуальные системы и их приложения. — 2016. — Т. 20, вып. 4. — С. 110–116.

7. Хинко Е. В. О несуществовании конструкций платовидных устойчивых булевых функций с некоторыми параметрами // Материалы XIII Международного семинара Дискретная математика и ее приложения имени академика О. Б. Лупанова (Москва, МГУ, 17–22 июня 2019 г.). — С. 326–329.

DOI: 10.20948/dms-2022-93