О расширении возможностей конструкции платовидных m-устойчивых булевых функций

Е. В. Хинко (МГУ имени М. В. Ломоносова, Москва)

Представлены новые возможности использования построенной ранее в [6] обеспечивающей рост устойчивости рекурсивной конструкции платовидных булевых функций с шагом числа переменных 3 с пересекающимися носителями спектра порождающих функций, приведён новый пример начальных функций.

Ключевые слова: булевы функции, корреляционная иммунность, устойчивость, платовидность, рекурсивные конструкции.

Вопрос корреляционной иммунности и устойчивости булевых функций имеет большое криптографическое значение и регулярно поднимается в работах многих авторов. Например, в [1] затрагивается проблема устойчивости функций при максимальных значениях нелинейности, а в работе [2] построены соответствующие конструкции функций. В [3] Ю. В. Таранниковым построены рекурсивные конструкции устойчивых булевых функций с высокой нелинейностью, где на каждом шаге рекурсии добавляется пара квазилинейных переменных. К относительно схожей теме в [4] также обращался К. В. Захаров, исследовавший рекурсивные конструкции бент-функций, которые можно считать подмножеством платовидных, с шагом числа переменных 2.

В большинстве из построенных ранее конструкций порождающие функции обладают непересекающимися носителями спектра. В [5] автором была построена рекурсивная конструкция платовидных устойчивых булевых функций с примерами начальных функций, где мощность пересечения носителей спектра всех четырёх функций равна четверти мощности носителя спектра каждой функции. В настоящей работе приводится расширение данной конструкции; показывается, что кроме соотношения 1 к 4 построенная в [5] конструкция допускает использование начальных функций с другими соотношениями мощности носителей спектров

всех 4 порождающих функций и носителя спектра каждой функции, а также приводится ссылка на пример других начальных функций с соотношением 5 к 8, показывающий, что существуют другие начальные функции с другими соотношениями мощности носителей спектров всех 4 порождающих функций и носителя спектра каждой функции.

Основные определения и факты

Приведём необходимые определения и основные факты о булевых функциях в соответствии с [2].

Обозначим за V_n множество двоичных векторов длины n. Рассмотрим булеву функцию $f : V_n \to F_2$; множество всех таких функций обозначим B_n. Скалярным произведением двух двоичных наборов $a, b \in V_n$ называется сумма по модулю 2 их покомпонентных произведений: $\langle a, b\rangle = \bigoplus_{i=1}^{n} a_i \cdot b_i$. Для каждого двоичного набора $u \in V_n$ определяется коэффициент Уолша:

$$W_f(u) = \sum_{x \in V_n} (-1)^{f(x)+\langle x,u\rangle}.$$

Вес набора $u \in V_n$ — число единиц в нём; обозначается $\mathrm{wt}(u)$. *Вес функции* $f \in B_n$ (обозначение $\mathrm{wt}(f)$) — количество наборов $u \in V_n$, для которых $f(u) = 1$. Функция $f \in B_n$ называется *уравновешенной*, если $\mathrm{wt}(f) = 2^{n-1}$.

Булева функция $f \in B_n$ называется *платовидной* (с амплитудой 2^c), если $W_f(u) \in \{0, \pm 2^c\}$ для всех $u \in V_n$, где $c \in \mathbb{N}$.

Функция $f \in B_n$ называется *корреляционно-иммунной порядка* m, $1 \leqslant m \leqslant n$, если $\mathrm{wt}(f') = \mathrm{wt}(f)/2^m$ для любой подфункции f' от $n - m$ переменных, то есть если значение f совокупность любых её m переменных статистически независимы. Обозначение: $f \in \mathrm{CI}(m)$. Функция f называется *m-устойчивой*, если $f \in \mathrm{CI}(m)$ и f уравновешена.

Носитель спектра функции f — множество $\{u \in V_n : W_f(u) \neq 0\}$.

Из определения коэффициентов Уолша видно, что для любой булевой функции f, носитель спектра её отрицания $\overline{f}$ совпадает с носителем спектра функции f, $W_{\overline{f}}(u) = W_f(u)$ для всех $u \in V_n$.

Равенство Парсеваля. *Для любой булевой функции f от n переменных имеет место равенство*

$$\sum_{u \in V_n} W_f^2(u) = 4^n. \tag{1}$$

Постановка задачи

В общем виде задачу исследования можно сформулировать так: пусть имеются b, $b \in \mathbb{N}$, платовидных m-устойчивых булевых функций от n переменных $f_n^i(x_1, x_2, \ldots, x_n)$, $i \in \{1, \ldots, b\}$, 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 $f_{n+3}^s(x_1, x_2, \ldots, x_n, x_{n+1}, x_{n+2}, x_{n+3})$, $s = 1, \ldots, 8$.

Будем рассматривать случай $b = 8$. Введём обозначение

$$\sigma_{sj} g_{sj} = \begin{cases} f_n^i, \sigma_{sj} = 1, \\ \overline{f_n^i}, \sigma_{sj} = -1, \end{cases}$$

где $s = 1, \ldots, 8$. Здесь σ_{sj} выполняет роль индикатора: выбирается функция или её отрицание.

Схематично связь между функциями от n и $n+3$ переменных мы можем записать так:

$$(f_{n+3}^s = \sigma_{s1} g_{s1} | \sigma_{s2} g_{s2} | \sigma_{s3} g_{s3} | \sigma_{s4} g_{s4} | \sigma_{s5} g_{s5} | \sigma_{s6} g_{s6} | \sigma_{s7} g_{s7} | \sigma_{s8} g_{s8}).$$

Пусть $a \in V_n$. Соотношения коэффициентов Уолша новых и старых функций можно кратко записать в матричном виде следующим образом:

$$(W_{f_{n+3}^s}(u000), \ldots, W_{f_{n+3}^s}(u111))^{\mathrm{T}} = \\ = M_3 \cdot (W_{g_{s1}}(u), W_{g_{s2}}(u), \ldots, W_{g_{s8}}(u))^{\mathrm{T}},$$

где M_3 — матрица Адамара — Сильвестра порядка 8.

Строки матрицы M_3 и наборы переменных $a \in V_n$ будем нумеровать с 1.

Представляет интерес подбор соотношений индикаторов σ_{sj} и порождающих функций f_n^i, чтобы построение новых функций от $n+3$ переменных с удовлетворяло следующим требованиям (рассматриваем случай $b = 8$):

(а) сохранение свойства платовидности;

(б) обеспечение роста устойчивости;

(в) возможность рекурсивного воспроизведения конструкции.

Конструкция

Обозначим через U_n пересечение носителей спектров всех b порождающих функций f_n^i, i=1, …, b. В [5] автором была построена конструкция

с примерами начальных функций для случая, когда восемь порождающих функций разбиваются на четыре пары совпадающих с точностью до отрицания функций, удовлетворяющая приведённым выше требованиям (а)–(в), где порождающие функции $f_n^i(x_1, x_2, \ldots, x_n)$, $i \in \{1, \ldots, b\}$, удовлетворяют следующим свойствам:

(К1) каждый двоичный набор $u \in V_n$ содержится в носителе спектра в точности нуля, двух или всех четырёх функций;

(К2) мощности всевозможных попарных пересечений носителей спектров порождающих функций f_n^i, $i = 1, \ldots, 4$, совпадают, а мощность пересечения носителей спектров всех четырёх функций U_n равна четверти мощности носителя спектра каждой функции;

(К3) для каждого набора $u \in V_n$, содержащегося в носителе спектра всех четырёх функций f_n^i, $i = 1, \ldots, 4$, коэффициенты Уолша трёх функций одного знака, а четвёртой — другого знака.

Очень естественно поставить вопрос, единственно ли соотношение 1 к 4 из критерия (К2)? На этот вопрос помогает ответить теорема.

Теорема 1. *Если отношение мощности U_n и мощности носителя спектра каждой порождающей функции $f_n^i, i = \overline{1,4}$ равно a к b, то отношение мощности U_{n+3} и мощности носителя спектра каждой порождающей функции $f_{n+3}^i, i = \overline{1,4}$ также равно a к b.*

Доказательство. Из (2) следует, что значение коэффициента Уолша новой функции $W_{f_{n+3}^s}(uu_{n+1}u_{n+2}u_{n+3})$ однозначно определяется значениями коэффициентов Уолша $W_{f_n^i}(u), i = 1, \ldots, 4$ порождающих функций на наборе a. Из доказанного в [5] следует, что

а) Ненулевые коэффициенты Уолша у новых функций могут быть только на наборах с чётными номерами ([5], лемма 1).

б) Если $W_{f_n^i}(u) \neq 0, i = \overline{1,4}, u \in U_n$, то, как следует из ([5], леммы 2, 3), $W_{f_{n+3}^i}(u001) \times W_{f_{n+3}^i}(u011) \times W_{f_{n+3}^i}(u101) \times W_{f_{n+3}^i}(u111) \neq 0, i = \overline{1,4}$, то есть если $u \in U_n$, то $\{u001, u011, u101, u111\} \subseteq U_{n+3}$.

в) Никакие другие наборы от $n+3$ переменных не входят в U_{n+3} ([5], лемма 4).

Таким образом, для каждого набора $u \in V_n$, лежащего в пересечении носителей спектров всех 4 порождающих функций $f_n^i, i = \overline{1,4}$, существует ровно 4 соответствующих ему ненулевых коэффициента Уолша у каждой новой функции $f_{n+3}^s, s = \overline{1,4}$, то есть если $\mid U_n \mid = a$, то $\mid U_{n+3} \mid = 4a$.

Из равенства Парсеваля (1) следует, что мощность носителя спектра каждой новой функции $f_{n+3}^i, i = \overline{1,4}$, в 4 раза больше мощности носителя

спектра каждой из порождающих $f^i_{n+3}, i = \overline{1,4}$, то есть если мощность спектра $f^i_n, i = \overline{1,4}$ равна b, то мощность спектра $f^s_{n+3}, s = \overline{1,4}$ равна $4b$. То есть отношение $\frac{a}{b} = \frac{4a}{4b}$ сохраняется. Теорема доказана.

Таким образом, могут существовать серии функций с любыми соотношениями между мощностью U_n и мощностью спектра каждой функции в зависимости от начальных условий, и свойство (K2) можно переписать следующим образом:

(K2) мощности всевозможных попарных пересечений носителей спектров порождающих функций f^i_n, $i = 1, \ldots, 4$, совпадают, *а соотношение мощности пересечения носителей спектров всех четырёх функций $f^i_n, i = \overline{1,4}$, и мощности носителя спектра каждой функции постоянно на каждом шаге.*

В качестве примера существования других соотношений (в дополнение к полученному в [5] соотношению 1 к 4) можно привести четыре 1-устойчивые функции от 5 переменных, построенные автором в [6]), удовлетворяющие новым критериям (K1)–(K3), для которых мощность пересечения носителей спектров всех четырёх функций f^i_n, $i = 1, \ldots, 4$, равна пяти восьмым мощности носителя спектра каждой функции.

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. — Springer-Verlag, 2001. — 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, Paris, January 8–12, 2001. Electronic Notes in Discrete Mathematics. — Elsever Science, 2001. — V. 6.

[3] Таранников Ю. В. О корреляционно-иммунных и устойчивых булевых функциях // Математические вопросы кибернетики. — 2002. — Вып. 11. — С. 91–148.

[4] Захаров К. В. О порождении бент-функций рекурсивными конструкциями / Дипломная работа. — М., 2008.

[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 двух новых рекурсивных конструкциях платовидных устойчивых булевых функций // Материалы XII Международного семинара «Дискретная математика и её приложения» имени академика О. Б. Лупанова (М., 20–25 июня 2016 г.). — С. 401–403