2013 Теоретические основы прикладной дискретной математики №1(19)

DOI 10.17223/20710410/19/2

УДК 519.7

О ВЕРХНЕЙ ОЦЕНКЕ НЕЛИНЕЙНОСТИ НЕКОТОРОГО КЛАССА БУЛЕВЫХ ФУНКЦИЙ С МАКСИМАЛЬНОЙ АЛГЕБРАИЧЕСКОЙ ИММУННОСТЬЮ[1]

Н. А. Коломеец

Институт математики СО РАН, г. Новосибирск, Россия

E-mail: nkolomeec@gmail.com

Доказывается верхняя оценка нелинейности булевых функций от чётного числа переменных, обладающих максимально возможной алгебраической иммунностью и предложенных D. K. Dalai и др. в 2006 г.

Ключевые слова: *булевы функции, нелинейность, алгебраическая иммунность.*

Введение

В работе [1] N. Courtois и W. Meier предложили метод криптоанализа шифров, основанных на фильтрующих генераторах. Этот криптоанализ использует следующие слабости фильтрующей функции: наличие у неё аннигиляторов низкой степени и множителей, существенно уменьшающих степень получающейся в результате произведения функции. В работе [2] сформулировано понятие алгебраической иммунности булевой функции, которое объединило эти слабости в одно свойство. Таким образом, булевы функции с низкой алгебраической иммунностью обладают слабостью к алгебраической атаке на поточные шифры.

В данной работе рассматривается верхняя оценка нелинейности булевых функций от чётного числа переменных, предложенных в [3].

Основная часть

Через $\mathbb{Z}_2^n$ обозначим n-мерный булев куб. Под *расстоянием* между двумя булевыми функциями будем понимать *расстояние Хэмминга* (число векторов, на которых функции различаются). *Вес Хэмминга* вектора x ($\mathrm{wt}(x)$) — количество его ненулевых координат. Будем называть i-м слоем n-мерного булева куба все векторы веса i.

Степень алгебраической нормальной формы булевой функции называется *алгебраической степенью* функции (обозначается $\deg(f)$). Булева функция называется *аффинной*, если её алгебраическая степень не превосходит 1.

Алгебраической иммунностью булевой функции f ($\mathrm{AI}(f)$) называют минимальную положительную алгебраическую степень булевой функции, которая аннулирует f или $f \oplus 1$, т. е.

$$\mathrm{AI}(f) = \min_{g \neq 0} \{\deg(g) : f(x)g(x) \equiv 0 \text{ или } (f(x) \oplus 1)g(x) \equiv 0\}.$$

Известно, что для функции f от n переменных $\mathrm{AI}(f) \leqslant \lceil n/2 \rceil$. Для криптографических приложений наибольший интерес представляют функции с максимально возможной алгебраической иммунностью, т. е. с $\mathrm{AI}(f) = \lceil n/2 \rceil$ (это значение достигается для любого n).

[1]Исследование выполнено при поддержке РФФИ, проект № 12-01-31097.

Рассмотрим нелинейность функций, обладающих максимальной возможной алгебраической иммунностью, а именно функций, построенных с помощью одной из самых простых конструкций для чётного числа переменных, которая предложена в работе [3]:

$$f(x) = \begin{cases} 0, & \mathrm{wt}(x) < n/2, \\ b(x) \in \{0,1\}, & \mathrm{wt}(x) = n/2, \\ 1, & \mathrm{wt}(x) > n/2. \end{cases} \tag{1}$$

Все такие функции обладают алгебраической иммунностью $n/2$.

Напомним, что нелинейностью булевой функции f (обозначается $\mathrm{nl}(f)$) называется расстояние Хэмминга от функции f до класса аффинных функций.

Известна следующая оценка снизу на нелинейность функции от n переменных [4]:

$$\mathrm{nl}(f) \geqslant 2 \sum_{i=0}^{\mathrm{AI}(f)-2} C_{n-1}^{i}.$$

Для булевых функций с максимально возможной алгебраической иммунностью от чётного числа переменных n эта оценка выглядит следующим образом:

$$\mathrm{nl}(f) \geqslant 2^{n-1} - 2C_{n-1}^{n/2}. \tag{2}$$

Среди функций вида (1) существуют такие, для которых в (2) достигается равенство. Эта оценка доказана также в [3] для функций вида (1), уравновешенных на среднем слое.

Докажем верхнюю оценку нелинейности для данного класса функций. Следует упомянуть, что данная оценка приводится (как тезис) в презентации Ch. Li [5].

Теорема 1. Для функций f вида (1) выполняется

$$\mathrm{nl}(f) \leqslant 2^{n-1} - C_{n-1}^{n/2}.$$

Доказательство. Оценим расстояния d_i от функций вида (1) до линейных функций $l_i(x) = x_i$, $i \in \{1, \ldots, n\}$, n — количество переменных. Пусть f — функция вида (1) от n переменных. Рассмотрим расстояния на каждом слое булева куба $\mathbb{Z}_2^n$ отдельно. Пусть d_i^j — расстояние до l_i на j-м слое, т .е.

$$d_i^j = \left|\{x \in \mathbb{Z}_2^n : \mathrm{wt}(x) = j, f(x) \neq l_i(x)\}\right|, j \in \{0, \ldots, n\}.$$

Тогда $d_i = d_i^0 + d_i^1 + \ldots + d_i^n$. Очевидно, что

$$d_i^j = \begin{cases} 0, & j = 0, \\ C_{n-1}^{j-1}, & 0 < j < n/2, \\ d_i^{n/2}, & j = n/2, \\ C_{n-1}^{j}, & n/2 < j < n, \\ 0, & j = n. \end{cases} \tag{3}$$

Поэтому

$$d_i = \sum_{j=1}^{n/2-1} C_{n-1}^{j-1} + \sum_{j=n/2+1}^{n-1} C_{n-1}^{j} + d_i^{n/2} = \sum_{j=0}^{n/2-2} C_{n-1}^{j} + \sum_{n/2+1}^{n-1} C_{n-1}^{j} + d_i^{n/2} =$$

$$= \sum_{j=0}^{n-1} C_{n-1}^{j} - C_{n-1}^{n/2-1} - C_{n-1}^{n/2} + d_i^{n/2} = 2^{n-1} - 2C_{n-1}^{n/2} + d_i^{n/2}.$$

Далее заметим, что для любого вектора x из среднего слоя ровно половина из l_i отличается от f на этом векторе x. Таким образом,

$$\sum_{i=1}^{n} d_i^{n/2} = n/2 \cdot C_n^{n/2} = n \cdot C_{n-1}^{n/2}.$$

Следовательно, существует i', такой, что

$$d_{i'}^{n/2} \leqslant C_{n-1}^{n/2},$$

т. е.

$$d_{i'} \leqslant 2^{n-1} - 2C_{n-1}^{n/2} + C_{n-1}^{n/2} = 2^{n-1} - C_{n-1}^{n/2}.$$

Теорема доказана. ■

В работе [3] доказано, что для функции

$$f(x) = \begin{cases} 0, & \mathrm{wt}(x) \leqslant n/2, \\ 1, & \mathrm{wt}(x) > n/2 \end{cases}$$

от n переменных выполняется

$$\mathrm{nl}(f) = 2^{n-1} - C_{n-1}^{n/2}.$$

Таким образом, оценка из теоремы 1 достигается.

Следствие 1. Для любой функций f вида (1) верно

$$2^{n-1} - 2C_{n-1}^{n/2} \leqslant \mathrm{nl}(f) \leqslant 2^{n-1} - C_{n-1}^{n/2},$$

при этом обе оценки достигаются.

Напомним, что максимально возможная нелинейность булевой функции от чётного числа переменных равна $2^{n-1} - 2^{n/2-1}$, т. е. нелинейность рассматриваемых функций весьма далека от максимально возможной.

ЛИТЕРАТУРА

1. *Courtois N. and Meier W.* Algebraic attacks on stream ciphers with liner feedback // LNCS. 2003. V. 2656. P. 345–359.
2. *Meier W., Pasalic E., and Carlet C.* Algebraic attacks and decomposition of Boolean functions // LNCS. 2004. V. 3027. P. 474–491.
3. *Dalai D.K., Maitra S., and Sarkar S.* Basic theory in construction of Boolean functions with maximum possible annihilator immunity // Designs, Codes and Cryptography. 2006. V. 40. Iss. 1. P. 41–58.
4. *Лобанов М. С.* Точное соотношение между нелинейностью и алгебраической иммунностью // Дискретная математика. 2006. Вып. 18. № 3. С. 152–159.
5. *Li Ch.* A survey on construction of Boolean function with optimum algebraic immunity (AI) // `http://www.frisc.no/wp-content/uploads/2011/10/Li-A-survey-on-constructions-of-BFs-with-optimum-AI.pdf`