

4. Зубков А. М., Серов А. А. Оценки числа булевых функций, имеющих аффинные приближения заданной точности // Дискретная математика. 2010. № 4. С. 3–19.

УДК 519.7

О НЕЛИНЕЙНОСТИ НЕКОТОРЫХ БУЛЕВЫХ ФУНКЦИЙ С МАКСИМАЛЬНОЙ АЛГЕБРАИЧЕСКОЙ ИММУННОСТЬЮ

Н. А. Коломеец

После публикации работ [1, 2] большое внимание уделяется алгебраической иммунности булевых функций. Алгебраическая иммунность булевой функции f (обозначается через $AI(f)$) — это минимальная положительная алгебраическая степень булевой функции, аннулирующей f или $f \oplus 1$, т. е.

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

Известно, что для функции f от n переменных $AI(f) \leq \lceil n/2 \rceil$. Для криптографических приложений наибольший интерес представляют функции с максимально возможной алгебраической иммунностью, т. е. с $AI(f) = \lceil n/2 \rceil$ (такое значение алгебраической иммунности достижимо для любого n).

В данной работе исследуется нелинейность функций, обладающих максимально возможной алгебраической иммунностью, а именно: рассматриваются функции, построенные с помощью одной из самых простых конструкций для чётного числа переменных, которая предложена D. K. Dalai и др. в работе [3]:

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

где n — количество переменных (n чётно); $\text{wt}(x)$ — вес Хэмминга вектора x . Все такие функции обладают алгебраической иммунностью $n/2$.

Нелинейностью булевой функции f (обозначается через $nl(f)$) называется расстояние Хэмминга от функции f до класса аффинных функций (функций вида $a_1x_1 \oplus \dots \oplus a_nx_n \oplus a_0$). Это также одно из важнейших криптографических свойств булевых функций.

Получена следующая верхняя оценка нелинейности функций вида (1).

Теорема 1. Для функций f вида (1) выполняется

$$nl(f) \leq 2^{n-1} - \binom{n-1}{n/2}.$$

В той же работе [3] рассматривается нелинейность функций, полученных с помощью данной конструкции, а именно доказано

Утверждение 1 (Dalai и др. [3]). Для функции

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

от n переменных (n чётно) верно

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

Таким образом, оценка из теоремы 1 достижима.

Поскольку максимальная нелинейность для функций от чётного числа переменных равна $2^{n-1} - 2^{n/2-1}$, нелинейность функций вида (1) заметно отличается от максимально возможной.

ЛИТЕРАТУРА

1. Courtois N. and Meier W. Algebraic Attacks on Stream Ciphers with Linear 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.

УДК 519.7

О СТАТИСТИЧЕСКОЙ НЕЗАВИСИМОСТИ СУПЕРПОЗИЦИИ БУЛЕВЫХ ФУНКЦИЙ. II

О. Л. Колчева, И. А. Панкратова

Следуя [1], будем говорить, что булева функция f статистически не зависит от подмножества U своих аргументов, если для любой её подфункции f' , полученной фиксированием значений всех переменных в U , имеет место $w(f') = w(f)/2^{|U|}$, где $w(f)$ — вес функции f .

В [2] доказано следующее утверждение.

Утверждение 1. Пусть x, y, z — переменные со значениями в $(\mathbb{Z}_2)^n$, $(\mathbb{Z}_2)^m$ и $(\mathbb{Z}_2)^l$ соответственно и функция $f(x, y)$ статистически не зависит от переменных в x . Тогда и функция $h(x, y, z) = g(f(x, y), z)$, где g — любая функция от $l + 1$ переменных, статистически не зависит от переменных в x .

В общем случае это утверждение не допускает обобщения на случай нескольких внутренних функций f . Получено следующее достаточное условие статистической независимости от аргументов суперпозиции произвольной функции с двумя внутренними функциями.

Утверждение 2. Пусть x, y, z — переменные со значениями в $(\mathbb{Z}_2)^n$, $(\mathbb{Z}_2)^m$ и $(\mathbb{Z}_2)^l$ соответственно, функции $f_1(x, y)$, $f_2(x, y)$, $u(x, y) = f_1(x, y) \oplus f_2(x, y)$ статистически не зависят от переменных в x . Тогда и функция $h(x, y, z) = g(f_1(x, y), f_2(x, y), z)$, где g — любая функция от $l + 2$ переменных, статистически не зависит от переменных в x .

Доказательство. Для любых $a \in \{0, 1\}^n$, $i, j \in \{0, 1\}$ обозначим $c_{ij}^a = |\{y \in \{0, 1\}^m : f_1(a, y) = i, f_2(a, y) = j\}|$. В силу статистической независимости функций f_1 , f_2 , u от переменных в x для любого $a \in \{0, 1\}^n$ выполняется

$$c_{10}^a + c_{11}^a = w(f_1)/2^n, \quad c_{01}^a + c_{11}^a = w(f_2)/2^n, \quad c_{01}^a + c_{10}^a = w(u)/2^n.$$

Отсюда получаем $c_{01}^a = (w(u) - w(f_1) + w(f_2))/2^{n+1}$, $c_{10}^a = (w(u) + w(f_1) - w(f_2))/2^{n+1}$, $c_{11}^a = (w(f_1) + w(f_2) - w(u))/2^{n+1}$, $c_{00}^a = 2^m - (w(u) + w(f_1) + w(f_2))/2^{n+1}$, т. е. c_{ij}^a не зависит от a для всех $i, j \in \{0, 1\}$. Тогда и вес подфункции функции h , полученной фиксацией переменных в x набором значений a , не зависит от a , так как $w(h(a, y, z)) =$