

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 $w(h(a, y, z)) =$

$= \sum_{i,j \in \{0,1\}} c_{ij}^a \cdot w(g(i, j, z))$. Следовательно, функция h статистически не зависит от переменных в x . ■

Следующее утверждение характеризует условия статистической независимости от переменных в x суммы двух функций в частном случае — когда одна из функций зависит только от x .

Утверждение 3. Пусть x, y — переменные со значениями в $(\mathbb{Z}_2)^n$ и $(\mathbb{Z}_2)^m$ соответственно и функция $f(x, y)$ статистически не зависит от переменных в x . Тогда функция $f(x, y) \oplus g(x)$, где g — любая функция от n переменных, статистически не зависит от переменных в x , если и только если f уравновешена или $g = \text{const}$.

Доказательство. По условию $w(f(a, y)) = w(f)/2^n$ для всех $a \in \{0, 1\}^n$; следовательно, $w(f(a, y) \oplus g(a))$ не зависит от a , если и только если $g = \text{const}$ или $w(f)/2^n = 2^m - w(f)/2^n$; последнее равенство равносильно уравновешенности f . ■

ЛИТЕРАТУРА

1. Агibalов Г. П., Панкратова И. А. Элементы теории статистических аналогов дискретных функций с применением в криптоанализе итеративных блочных шифров // Прикладная дискретная математика. 2010. № 3(9). С. 51–68.
2. Колчева О. Л., Панкратова И. А. О статистической независимости суперпозиции булевых функций // Прикладная дискретная математика. Приложение. 2011. № 4. С. 11–12.

УДК 519.712.2

ОБ ОДНОЙ ЗАДАЧЕ КОМБИНАТОРНОЙ ОПТИМИЗАЦИИ¹

А. С. Кузнецова, К. В. Сафонов

Пусть есть n стульев, каждый из которых имеет уникальный порядковый номер $i = 1, 2, \dots, n$. Стулья расставлены по окружности. На стулья произвольным образом садятся n человек так, что на каждом стуле оказывается по одному человеку. Каждый человек имеет уникальный порядковый номер $j = 1, 2, \dots, n$. Посадка называется правильной, если у всех стульев порядковые номера совпадают с номерами сидящих на них людей, в противном случае посадка называется неправильной. Будем называть перестановкой перемену мест двух сидящих рядом людей. Требуется вычислить наименьшее число перестановок d , которые позволят получить правильную посадку из произвольной начальной посадки.

Перестановки (p, q) , указанные в условии задачи, порождают симметрическую группу S_n степени n . Запишем данную группу через порождающие элементы и определяющие соотношения. Пусть $x_1 = (1, 2)$, $x_2 = (2, 3)$, ..., $x_{n-1} = (n-1, n)$, $x_n = (1, n)$ — порождающие элементы группы S_n . Теперь запишем определяющие соотношения R для S_n :

$$R = \begin{cases} x_i^2 = e, & i = 1, 2, \dots, n, \\ (x_i x_j)^2 = e, & \text{если } 1 < |j - i| < n - 1, \\ (x_i x_j)^3 = e, & \text{если } |j - i| = 1 \text{ или } |j - i| = n - 1, \\ x_1 x_2 \dots x_{n-2} x_{n-1} x_{n-2} \dots x_2 x_1 = x_n. \end{cases}$$

Таким образом,

$$S_n = \langle x_1, x_2, \dots, x_n \mid R \rangle.$$

¹Работа поддержана грантом РФФИ, проект № 10-01-00509-а.