Секция «Дискретная математика и математическая кибернетика»

О новых рекурсивных конструкциях с шагом числа переменных три платовидных устойчивых булевых функций

Хинко Евгений Викторович

Аспирант

Московский государственный университет имени М.В.Ломоносова,
Механико-математический факультет, Кафедра дискретной математики, Москва, Россия

E-mail: khinko-eugene@ya.ru

Вопрос корреляционной иммунности и устойчивости булевых функций имеет большое криптографическое значение и регулярно поднимается в работах многих авторов. Например, в [3] затрагивается проблема устойчивости функций при максимальных значениях нелинейности, а в работах [4] построены соответствующие конструкции функций. В [1] 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 [2] также обращался К. В. Захаров, исследовавший рекурсивные конструкции бент-функций с шагом числа переменных 2.

***

Задачу проделанной работы можно в общей формулировке поставить 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}. Представляет интерес подбор таких новых функций от $n+3$ переменных ($f_{n+3}^s(x_1, x_2, \ldots, x_n, x_{n+1}, x_{n+2}, x_{n+3})$, $s = 1, \ldots, 8.$), которые удовлетворяют следующим условиям: а) сохранение свойства платовидности; б) обеспечение роста устойчивости; в) рекурсивное воспроизведение конструкции. В настоящей работе получены рекурсивные конструкции платовидных булевых функций с шагом числа переменных 3, удовлетворяющие данным условиям, и приведены примеры начальных функций. Отличительной особенностью построенных конструкций является то, что рассматривался случай порождающих функций с пересекающимися носителями спектра, в то время как большинстве из построенных ранее конструкций порождающие функции обладали непересекающимися носителями спектра.

Источники и литература

1) Таранников Ю. В. О корреляционно-иммунных и устойчивых булевых функциях,// Математические вопросы кибернетики, вып. 11, 2002, с.˜91–148.

2) Захаров К.В., О порождении бент-функций рекурсивными конструкциями // Дипломная работа, М, 2008.

3) 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. – Springer-Verlag. – 2001.

4) 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. – V.6. – Elsever Science. – 2001.