

ОБ АФФИННОЙ РАСЩЕПЛЯЕМОСТИ НЕКОТОРЫХ КЛАССОВ БУЛЕВЫХ ФУНКЦИЙ

Бабуева Александра Алексеевна

Студент

Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия

E-mail: sasha.babueva@gmail.com

В теории кодирования и криптографии линейная (аффинная) аппроксимация исследуемых функций рассматривается как необходимый этап сведения исходной задачи к решению систем линейных уравнений. Переход к системе линейных уравнений свидетельствует о возможности построения эффективного алгоритма решения исходной задачи. Одним из важных параметров, характеризующих возможность линейной аппроксимации функции, является свойство аффинной расщепляемости.

Свойство аффинной расщепляемости по некоторому подпространству [2] говорит о том, что сужение булевой функции на любой сдвиг этого подпространства совпадает с некоторой аффинной функцией. Если функция является аффинно расщепляемой, то задача ее исследования заметно упрощается.

Была показана аффинная расщепляемость некоторых классов функций, используемых для синтеза криптографических отображений, обладающих свойствами максимальной нелинейности, корреляционной иммунности и другими криптографическими свойствами, характеризующими устойчивость отображения к определенным криптографическим атакам.

Для построения корреляционно-иммунных функций с заданными криптографическими свойствами зачастую используются алгебраически вырожденные функции. Булева функция f от n переменных называется *алгебраически вырожденной*, если существует матрица D — $(n \times k)$, $k < n$ и булева функция g от k переменных такие, что

$$f(x) \equiv g(xD).$$

Теорема 1. *Если булева функция f алгебраически вырожденная порядка $n - k$, то она аффинно расщепляема порядка k .*

Для синтеза максимально нелинейных функций может использоваться конструкция Мэйорана–Мак–Фарланда [4].

Теорема 2. *Функции из класса Мэйорана–Мак–Фарланда являются аффинно расщепляемыми.*

Для синтеза корреляционно-иммунных функций также может использоваться конструкция линейного разветвления. Булева функция f задана в виде линейного разветвления, если существуют такие $t, s, n = t + s, \Phi \in \mathcal{F}_{s,t}, h \in \mathcal{F}_s$, что

$$f(z) = f(x, y) = \langle x, \Phi(y) \rangle \oplus h(y) \quad (1)$$

для любых $z = (x, y) \in V_n, x \in V_t, y \in V_s$.

Теорема 3. *Функции, заданные в виде (1), являются аффинно расщепляемыми.*

Было показано, что для построения фильтрующих генераторов применяются аффинно расщепляемые функции. Кроме того, было показано, что при синтезе m -устойчивых функций, нелинейность которых достигает максимального значения [3], также используются аффинно расщепляемые функции.

Были получены соотношения между порядком аффинной расщепляемости функции и ее индексом линейности и уровнем аффинности (введено в работе [1]). Если булева функция f от n переменных является аффинно расщепляемой порядка k , то ее уровень аффинности $la(f) = n - k$. Если индекс линейности отображения равен k , то оно аффинно расщепляемо порядка $n - k$.

Литература

1. Буряков М.Л., Логачев О.А.. *Об уровне аффинности булевых функций*. Дискрет. матем., 2005, том 17, выпуск 4, 98–10
2. Коломеев Н. А. Бент-функции, аффинные на подпространствах, и их метрические свойства. Дисс. ... ученой степени канд. физ.-мат. наук, Институт математики им. С.Л. Соболева СО РАН, Новосибирск 2014, С. 68.
3. Таранников Ю. В. *О корреляционно-иммунных и устойчивых булевых функциях*. Матем. вопросы кибернетики (2002) 11, 91–148.
4. McFarland, R.I. *A family of difference sets in non-cyclic groups*. J. Comb. Theory Ser. A. 15, 1–10(1973)