О связи алгебраических, комбинаторных и криптографических свойств булевых функций и их сужений

Бабуева Александра Алексеевна

Студент

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

E-mail: sasha.babueva@gmail.com

Понятие сужения булевой функции активно используется как в синтезе, так и в анализе криптографических функций. В качестве основных причин исследований этого понятия можно назвать следующие:

- анализ свойств булева отображения удобно проводить, используя семейство сужений этого отображения на специальным образом подобранное множество областей;
- тесная связь свойств сужений и исходного булева отображения (в том числе и наследование свойств).

В работе исследовались свойства сужений бент-функций и аффинно-расщепляемых функций. Бент-функцию можно определить как функцию, которая плохо аппроксимируется аффинными функциями. В блочных и поточных шифрах бент-функции и их векторные аналоги используются для синтеза криптографических отображений, устойчивых к ряду методов криптографического анализа. Свойство аффинной расщепляемости по некоторому подпространству (введено в работе [1]) говорит о том, что сужение булевой функции на любой сдвиг этого подпространства совпадает с некоторой аффинной функцией. Если криптографическая функция является аффинно-расщепляемой, то задача ее исследования заметно упрощается. Поэтому исследование сужений именно бент-функций и аффинно-расщепляемых функций, а также вопрос о том, может ли бент-функция быть аффинно-расщепляемой, представляет особый интерес. В работе рассматривались такие параметры булевых функций, как нелинейность, алгебраическая степень, спектр Уолша–Адамара, нормальность, слабая нормальность.

Были получены следующие результаты:

- доказано соотношение, связывающее величины квадратов коэффициентов неполного преобразования Уолша–Адамара

функции на смежных классах по подпространству с квадратом коэффициентов Уолша–Адамара исходной функции (сформулировано в [2]);

- доказано равенство «нулевых» коэффициентов неполного преобразования Уолша–Адамара бент-функции и дуальной к ней функции;
- доказано, что если бент-функция нормальна (слабо нормальна), то и дуальная ей функция нормальна (слабо нормальна);
- получена верхняя оценка алгебраической степени аффинно-расщепляемой функции:

  Теорема 1. *Пусть $f \in \mathcal{F}_n$ – аффинно-расщепляемая по подпространству L функция, $dimL = r$. Тогда $deg(f) \leq n - r + 1$.*

- доказано, что свойство аффинной расщепляемости инвариантно относительно полной аффинной группы;
- получены достаточные условия аффинной расщепляемости дуальной бент-функции;
- получена верхняя оценка нелинейности булевой функции, обладающей нетривиальным пространством линейных трансляторов (структур):

  Теорема 2. *Пусть $f \in \mathcal{F}_n$ имеет линейную структуру: $dimL_f = r$. Тогда $nl(f) \leq 2^{n-1} - 2^{\frac{n-r}{2}-1}$.*

Литература

1. Коломеец 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.
2. Logachev O. A., Yashchenko V. V., Denisenko M. P. Local Affinity of Boolean Mappings. // In Boolean functions in cryptology and information security, NATO science for peace and security series, D: information and communication security - vol. 18, ed. by Preneel B., Logachev O. A., IOS Press, 2008, P. 148–172.