УДК 519.651

НЕКОТОРЫЕ СВОЙСТВА ГИПЕР-БЕНТ-ФУНКЦИЙ

Асп. ***Датиев М.К.***, ст. н.с. ***Иванов А.В.***, проф. ***Датиев К.М.***
Северо-Кавказский горно-металлургический институт.
Московский институт радиотехники, электроники и автоматики

Рассматривается специальный класс булевых функций – гипер-бент-функций. Данный класс функций обладает рядом стойких криптографических свойств. Для определения принадлежности произвольного отображения к классу гипер-бент-функций был разработан соответствующий алгоритм. Проведены эксперименты с булевыми функциями, на основании результатов которых доказаны утверждения, описывающие новые свойства гипер-бент-функций.

Булевы функции играют значительную роль в прикладных областях математики. Гипер-бент-функции (ГБФ) – это специальный класс булевых функций, впервые описанный в работе [1] Йозефом и Гонгом. Данный класс функций обладает стойкими криптографическими свойствами, что позволяет использовать гипер-бент-функции во многих областях криптографии.

При анализе криптографических алгоритмов, построенных с использованием преобразований конечных полей, часто появляется необходимость найти эффективное приближение некоторой функции, заданной на конечном поле, в определенном множестве функций – классе приближений [2].

Известно, что вероятность совпадения значений любой булевой функции от n переменных со значениями ее лучшей аффинной аппроксимации не меньше величины $\frac{1}{2}+2^{-\frac{n}{2}-1}$ [3]. Функции, для которых эта оценка обращается в равенство, были названы О.С. Ротхаузом «бент-функциями».

При изучении свойств булевых функций от n переменных, рассмотрение их представлений в виде многочленов от одной переменной над полем $\mathrm{GF}\left(2^n\right)$ позволяет использовать соответствующий алгебраический аппарат [3]. В работе [4] для

одного из таких представлений был использован термин «приведенное представление в базисе векторного пространства $\mathrm{GF}\left(2^n\right)_{\mathrm{GF}(2)}$». В работе [4] изучен класс так называемых собственных мономиальных функций, заданных приведенными представлениями в базисе пространства $\mathrm{GF}\left(2^n\right)_{\mathrm{GF}(2)}$, двойственном к некоторому полиномиальному базису. Показано, что для бент-функций от n переменных степени нелинейности не выше $\frac{n}{2}-1$ в данном классе существует более точное приближение, чем в классе линейных функций. В работе [1] построен класс отображений из поля $\mathrm{GF}\left(2^n\right)$ в поле $\mathrm{GF}(2)$, который наихудшим образом приближается как линейными функциями, так и собственными мономиальными функциями. В настоящее время такие отображения называются «гипер-бент-функциями» [1; 4].

Обозначим через F_n – множество всех отображений поля $\mathrm{GF}\left(2^n\right)$ в поле $\mathrm{GF}(2)$. Для того чтобы определить, является ли $F \in \mathrm{F}_n$ гипер-бент-функцией, необходимо найти коэффициенты расширенного преобразования Уолша-Адамара, то есть посчитать расстояние до всех функций вида $tr_1^n(ax^\delta)$, где $a \in Q,\ (\delta, 2^n-1)=1$. Для наиболее эффективного нахождения коэффициентов расширенного преобразования Уолша-Адамара для любого $\delta:\ (\delta, 2^n-1)=1$ был разработан соответствующий алгоритм:

Алгоритм 1

1. Для заданного $\delta:(\delta, 2^n-1)=1$ *найти с помощью расширенного алгоритма Евклида соответствующее значение* $\sigma:\sigma\cdot\delta\equiv 1(\mathrm{mod}\,2^n-1)$.

2. Вычислить значения функции $F_\sigma(x)=F(x^\sigma)$.

3. С помощью быстрого преобразования Фурье найти коэффициенты Фурье для функции $F_\sigma(x)$.

4. Определить соответствующие коэффициенты преобразования Уолша-Адамара.

Найденные при помощи алгоритма 1 коэффициенты будут равны соответствующим коэффициентам расширенного преобразования Уолша-Адамара для функции $F \in \mathrm{F}_n$.

Если для всех $\delta : (\delta, 2^n - 1) = 1$ соответствующие коэффициенты расширенного преобразования Уолша-Адамара по абсолютной величине все будут равны $2^{\frac{n}{2}}$, можно сделать вывод, что функция $F \in \mathrm{F}_n$ является гипер-бент-функцией.

В работе [5] было экспериментально установлено, что любая булева функция φ от $n = 6$ переменных $\deg \varphi = 3$, являющаяся бент-функцией, эквивалентна с точностью до невырожденных аффинных замен переменных и добавления произвольных аффинных функций одной из следующих трех функций:

$$f = x^{(1)}x^{(2)}x^{(3)} \oplus x^{(1)}x^{(4)} \oplus x^{(2)}x^{(5)} \oplus x^{(3)}x^{(6)}; \quad (1)$$

$$g = x^{(1)}x^{(2)}x^{(3)} \oplus x^{(2)}x^{(4)}x^{(5)} \oplus x^{(1)}x^{(2)} \oplus x^{(1)}x^{(4)} \oplus x^{(2)}x^{(6)} \oplus \quad (2)$$
$$\oplus x^{(3)}x^{(5)} \oplus x^{(4)}x^{(5)};$$

$$h = x^{(1)}x^{(2)}x^{(3)} \oplus x^{(2)}x^{(4)}x^{(5)} \oplus x^{(3)}x^{(4)}x^{(6)} \oplus x^{(1)}x^{(4)} \oplus x^{(2)}x^{(6)} \oplus \quad (3)$$
$$\oplus x^{(3)}x^{(4)} \oplus x^{(3)}x^{(5)} \oplus x^{(3)}x^{(6)} \oplus x^{(4)}x^{(5)} \oplus x^{(4)}x^{(6)}.$$

Исследовался вопрос, бент-функциям какого из этих классов соответствуют в различных базисах бент-функции, являющиеся гипер-бент-функциями. В результате проведенных экспериментов был получен результат, показывающий, что только в третьем классе существуют бент-функции, соответствующие в некотором базисе гипер-бент-функциям.

На основании проведенных экспериментов были доказаны два утверждения, которые описывают новые свойства отображений из множества F_n, соответствующих одной булевой функции в специальным образом подобранных базисах.

Утверждение 1. Пусть θ – примитивный элемент поля Q. Пусть булева функция $\varphi\left(x^{(0)}, x^{(1)}, ..., x^{(n-1)}\right)$ соответствует в базисе $\vec{\varepsilon} = (1, \theta, \theta^2, ..., \theta^{n-1})$ векторного пространства Q_P

отображению $F(x)$, а в базисе $\overrightarrow{\varepsilon^*} = (\theta^i, \theta^{i+1}, \theta^{i+2}, ..., \theta^{i+n-1}), i \geq 0$ отображению $F^*(x)$. Тогда $F(x)$ является гипер-бент-функцией тогда и только тогда, когда $F^*(x)$ является гипер-бент-функцией.

Утверждение 2. Пусть θ – примитивный элемент поля Q. Пусть булева функция $\varphi\left(x^{(0)}, x^{(1)}, ..., x^{(n-1)}\right)$ соответствует в базисе $\vec{\varepsilon} = (1, \theta, \theta^2, ..., \theta^{n-1})$ векторного пространства Q_P отображению $F(x)$, а в базисе $\overrightarrow{\varepsilon^*} = (1, \theta^d, \theta^{2d}, ..., \theta^{d(n-1)})$, где $d = 2^t$ $(t \geq 1)$, отображению $F^*(x)$. Тогда $F(x)$ является гипер-бент-функцией тогда и только тогда, когда $F^*(x)$ является гипер-бент-функцией.

ЛИТЕРАТУРА

1. *Youssef A., Gong G.* Hyper-bent-functions // Advances in Cryptology. Proc. Of Eurocrypt'2001 // Lecture Notes in Computer Science. 2001. V. 2045. P. 406-419.

2. *Амбросимов А.С.* О приближении функций *k*-значной логики функциями из заданной системы // Фундаментальная и прикладная математика. 1997. Т. 3, вып. 3. С. 653-674.

3. *Лидл Р., Нидеррайтер Г.* Конечные поля. Т 1, 2. М.: Мир, 1988. 818 с.

4. *Кузьмин А.С., Марков В.Т., Нечаев А.А., Шишков А.Б.* Приближение булевых функций мономиальными // Дискретная математика. 2006. Т. 18, №1. С. 9–29.

5. Rothaus O. S. *On "Bent" Functions // Journal of Combinatorial Theory (A). V. 20. № 3. P. 300–305. 1976.*