Бент-функции

Бент-функции – это булевы функции обладающие экстремальным значением нелинейности. Мера нелинейности является важной характеристикой булевой функции в криптографии. Линейность и близкие к ней свойства часто свидетельствуют о простой (в определённом смысле) структуре этой функции и, как правило, представляют собой богатый источник информации о многих других ее свойствах.

Впервые бент-функции были введены О. Ротхаусом в 60-х годах XX века. Также к числу первых работ относятся и исследования американских математиков Дж. Диллона и Р.Л МакФарланда, которые в 70-х рассматривали бент-функции в связи с разностными множествами. С 80-х годов бент-функции начинают интенсивно изучатся по всему миру. В настоящее время известны сотни работ о бент-функциях и близких вопросах.

Несмотря на широкий интерес среди исследователей, класс бент-функций от n переменных до сих пор не описан, для мощности этого класса не найдена асимптотика и не установлено даже приемлемых нижних и верхних оценок. Проблемой является классификация бент-функций (от 10, 12 и т.д. переменных). Есть практическая потребность в изобретении новых конструкций бент-функций и эффективных алгоритмов генерации всех бент-функции.

Рассмотрим основные определения и результаты связанные с понятием бент-функции. V_n - векторное пространство размерности n над 2-хэлементным полем F_2. $a = (a_1, \ \dots, \ a_n)$, $b = (b_1, \ \dots, \ b_n)$, $a, \ b \in V_n$. Определим скалярное умножение на векторах из V_n: $\langle a, \ b \rangle = a_1 b_1 \oplus \dots \oplus a_n b_n$. Пусть $f: \ V_n \to F_2$ - булева функция.

Определение. Вес Хэмминга булевой функции f:

$$wt(f) = |\{x \in V_n : f(x) = 1\}|$$

Определение. Расстояние Хэмминга между двумя булевыми функциями f и g:

$$d(f, \ g) = wt(f \oplus g)$$

Определение. Аффинная функция – это булева функция, полином Жегалкина которой имеет вид:

$$a_1 x_1 \oplus \dots \oplus a_n x_n \oplus \mathrm{c}$$

A_n - класс аффинных функций над V_n.

Определение. Нелинейность булевой функции определим как:

$$N_f = \min_{\varphi \in A_n} d(f, \varphi)$$

Определение. Преобразование Уолша-Адамара булевой функции f есть функция $W_f(u)$: $V_n \to \mathbb{Z}$, задаваемое равенством:

$$W_f(u) = \sum_{x \in V_n} (-1)^{f(x) \oplus \langle x,\, u \rangle},\ u \in V_n$$

Теорема (равенство Парсеваля). Для любой булевой функции f справедливо равенство:

$$\sum_{u \in V_n} \left(W_f(u)\right)^2 = 2^{2n}$$

Теорема. Нелинейность булевой функции f и соответствующее преобразование Уолша-Адамара связаны соотношением:

$$N_f = 2^{n-1} - \frac{1}{2} \max_{u \in V_n} \left|W_f(u)\right|$$

Определение. Бент-функция f – булева функция от n переменных (n - четно) такая, что:

$$\forall u \in V_n \quad \left|W_f(u)\right| = 2^{n/2}$$

Примеры бент-функций для $n = 2$

$$x_1 x_2 \oplus x_1 \oplus x_2 \oplus 1$$

$$x_1 x_2 \oplus x_1 \oplus 1$$

$$x_1 x_2 \oplus x_2 \oplus 1$$

$$x_1 x_2 \oplus 1$$

$$x_1 x_2$$

$$x_1 x_2 \oplus x_2$$

$$x_1 x_2 \oplus x_1$$

$$x_1 x_2 \oplus x_1 \oplus x_2$$