О булевых функциях с мощностью множества критерия распространения, равной $2^n - 2$

Г.А. Исаев

***Аннотация*—Изучение критерия распространения и его свойств является одним из важнейших направлений исследований в области криптографических приложений булевых функций. Булева функция удовлетворяет критерию распространения по направлению (определяемому вектором из соответствующего n-мерного булева пространства), если производная данной функции по этому направлению является уравновешенной функцией. Совокупность всех таких направлений (векторов) для булевой функции называют множеством её критерия распространения.**

Необходимо отметить, что для некоторых классов булевых функций критерий распространения связан с их экстремальными свойствами. Например, количество векторов, удовлетворяющих критерию распространения, максимально лишь при чётном числе переменных и для экстремального класса булевых функций, называемых бент-функциями.

В работе рассматривается вопрос существования булевых функций, близких с точки зрения критерия распространения к бент-функциям, то есть таких функций, у которых все векторы, кроме нулевого и одного некоторого ненулевого вектора, удовлетворяют критерию распространения. Показано, что множество булевых функций с таким свойством существует только при нечётном числе переменных. Кроме того, изучен вопрос принадлежности множества булевых функций с этим свойством к каким-либо криптографическим классам и, в том числе, к классам корреляционно-иммунных и устойчивых функций, а также выявлено взаимно однозначное соотношение между этими функциями и бент-функциями.

***Ключевые слова*—булева функция, критерий распространения, уравновешенность, корреляционно-иммунная функция, устойчивая функция, спектр Уолша, автокорреляционная функция**

I. Введение

Среди основных криптографических характеристик булевых функций, необходимых для конструирования систем преобразования информации, определённый интерес представляет так называемый критерий распространения. Множество критерия распространения для булевой функции представляет собой понятие, описывающее направления, по которым производные являются уравновешенными функциями. Оно характеризует статистические свойства семейства производных булевой функции, играющих важную роль в анализе и синтезе криптосистем. Понятие критерия распространения было введено Бартом Пренелем и соавторами в [6] в целях характеризации стойкости криптографических систем относительно линейных и разностных методов криптоанализа, которые могут давать много информации о секретном ключе (подробнее об этих методах см. [2] и [3]). Помимо этого, для некоторых классов булевых функций критерий распространения связан с их экстремальными свойствами. Например, для максимально-нелинейных булевых функций (или бент-функций) множество критерия распространения содержит в себе все ненулевые векторы из соответствующего n-мерного булева пространства, в то время как для аффинных функций оно не содержит в себе ни одного вектора.

В данной работе рассматривается вопрос существования булевых функций, близких с точки зрения критерия распространения к бент-функциям, то есть таких функций, у которых все векторы, кроме нулевого и одного некоторого ненулевого вектора, удовлетворяют критерию распространения. Показано, что множество булевых функций с таким свойством существует только при нечётном числе переменных. Кроме того, изучен вопрос принадлежности множества булевых функций с этим свойством к каким-либо криптографическим классам и, в том числе, к классам корреляционно-иммунных и устойчивых функций, а также выявлено взаимно однозначное соотношение между этими функциями и бент-функциями.

II. Основные определения и обозначения

Пусть $\mathbb{F}_2$ — конечное поле, состоящее из двух элементов, $V_n = \mathbb{F}_2^n$ — векторное пространство наборов длины n с компонентами из поля $\mathbb{F}_2$. ***Булевой функцией*** от n переменных называется отображение из V_n в $\mathbb{F}_2$. Множество всех булевых функций от n переменных обозначим через $\mathcal{F}_n$.

Операции сложения и умножения элементов поля $\mathbb{F}_2$ будем обозначать соответственно через «$\oplus$» и «$\cdot$» (далее мы часто будем опускать знак «$\cdot$»: $ab = a \cdot b$).

Определим следующие операции над векторами из V_n:

- $a \oplus b = (a_1 \oplus b_1, \ldots, a_n \oplus b_n)$ — побитовое сложение

Статья получена 28 ноября 2022 г.

Глеб Андреевич Исаев, Московский государственный университет имени М.В. Ломоносова, факультет вычислительной математики и кибернетики (e-mail: gleb-isaev52@yandex.ru).

векторов $a, b \in V_n$,

- $a \oplus S = \{a \oplus u \colon u \in S\} \subset V_n$ — сложение вектора $a \in V_n$ и подпространства $S \subset V_n$,
- $\langle a, b \rangle = a_1 b_1 \oplus \cdots \oplus a_n b_n$ — скалярное произведение векторов $a, b \in V_n$.

Множество $C \subseteq V_n$ называется ***аффинным подпространством*** размерности k, если $C = a \oplus S$, где $a \in V_n$ и $S \subseteq V_n$ — линейное подпространство размерности k.

Произвольную булеву функцию f из $\mathcal{F}_n$ можно представить (см. [2]) в форме полинома от n переменных, т. е.

$$f(x_1, x_2, \ldots, x_n) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_n x_n \oplus$$

$$\oplus\, a_{12} x_1 x_2 \oplus a_{13} x_1 x_3 \oplus \cdots \oplus a_{1\ldots n} x_1 \ldots x_n,$$

где $a_{i_1 \ldots i_j} \in \mathbb{F}_2$, $j = 1, 2, \ldots, n$. Такое представление функции называется ***полиномом Жегалкина*** или ***алгебраической нормальной формой (АНФ)***. Выражение $x_{i_1} \ldots x_{i_j}$, $j = 1, 2, \ldots, n$ (когда $a_{i_1 \ldots i_j} = 1$) в полиноме Жегалкина функции f называется ***слагаемым в полиноме Жегалкина*** функции f. Число переменных в самом длинном слагаемом полинома Жегалкина функции f называется ***алгебраической степенью*** функции f и обозначается через $\deg f$. Если функция имеет степень не выше 1, то она называется *аффинной*.

Преобразованием Уолша–Адамара булевой функции f из $\mathcal{F}_n$ ([2]) называют целочисленную функцию W_f, задаваемую на множестве V_n равенством

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

Носителем спектра Уолша булевой функции f называется множество $SW_f = \{x \in V_n \colon W_f(x) \neq 0\}$.

Вес Хэмминга $wt(x)$ вектора $x = (x_1, \ldots, x_n)$ — это число ненулевых координат x_i. ***Вес*** $wt(f)$ ***булевой функции*** f определяется равенством

$$wt(f) = \#\{x \in V_n \colon f(x) = 1\},$$

где решётка «#» обозначает мощность соответствующего конечного множества.

Булева функция $f \in \mathcal{F}_n$ называется ***уравновешенной***, если $wt(f) = 2^{n-1}$.

Расстоянием Хэмминга между двумя функциями f и g из $\mathcal{F}_n$ называется число, задаваемое выражением $dist(f, g) = wt(f \oplus g)$.

Нелинейность $nl(f)$ булевой функции $f \in \mathcal{F}_n$ — это расстояние от f до множества аффинных функций $\mathcal{A}_n \subset \subset \mathcal{F}_n$:

$$nl(f) = dist(f, \mathcal{A}_n) = \min_{l \in \mathcal{A}_n} \left(dist(f, l) \right).$$

Обычно для вычисления этого параметра пользуются соотношением

$$nl(f) = 2^{n-1} - \frac{1}{2} \cdot W_{max},$$

где $W_{max} = \max_{u \in V_n} \left(|W_f(u)| \right)$.

Производной по направлению $u \in V_n$ функции $f \in \in \mathcal{F}_n$ называется булева функция $D_u f(x) = f(x) \oplus f(x \oplus \oplus u)$, где $x \in V_n$.

Автокорреляционной функцией булевой функции $f \in \mathcal{F}_n$ называется функция $\Delta_f(u)$, имеющая вид

$$\Delta_f(u) = \sum_{x \in V_n} (-1)^{f(x) \oplus f(x \oplus u)} = \sum_{x \in V_n} (-1)^{D_u f(x)}.$$

Матрицей Адамара–Сильвестра называется квадратная $(2^n \times 2^n)$-матрица H_n (n — натуральное) такая, что

$$H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \; H_n = \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix} \text{ для } n > 1.$$

Матрица H_n обладает следующими легко проверяемыми свойствами:

1. $H_n = H_n^\top$. В частности, $H_n H_n^\top = 2^n E_{2^n}$, где E_{2^n} — единичная $(2^n \times 2^n)$-матрица.
2. $H_n = (h_{u,v}) = \left((-1)^{\langle u, v \rangle} \right)$, где $u, v \in V_n$ — двоичное представление соответственно номеров строк и столбцов матрицы H_n.

Связь между спектром Уолша булевой функции и её автокорреляционной функцией характеризует следующая теорема.

Теорема 1 (о взаимной корреляции [2]). *Пусть* $f \in \in \mathcal{F}_n$. *Тогда*

$$\left(\Delta_f(0^n), \ldots, \Delta_f(1^n)\right) H_n = \left(W_f^2(0^n), \ldots, W_f^2(1^n)\right).$$

Непосредственно из теоремы о взаимной корреляции и свойств матрицы Адамара–Сильвестра вытекает очевидное утверждение.

Следствие 1 ([2]). *Пусть* $f \in \mathcal{F}_n$. *Тогда*

$$2^n \left(\Delta_f(0^n), \ldots, \Delta_f(1^n)\right) = \left(W_f^2(0^n), \ldots, W_f^2(1^n)\right) H_n.$$

В частности, справедливо равенство Парсеваля

$$\sum_{x \in V_n} W_f^2(x) = 2^{2n}.$$

Бент-функцией называется такая булева функция $f \in \mathcal{F}_n$ (n чётно), что модуль каждого коэффициента Уолша–Адамара W_f этой функции равен $2^{\frac{n}{2}}$. Множество всех бент-функций от n переменных будем обозначать через $\mathcal{B}_n$.

Говорят, что булева функция $f \in \mathcal{F}_n$ удовлетворяет ***критерию распространения*** по направлению $u \in \in V_n$, если производная $D_u f$ — уравновешенная функция (что эквивалентно условию $\Delta_f(u) = 0$). Множество всех таких векторов будем обозначать через $E_{PC}(f) = = \{u \in V_n \colon wt(D_u f) = 2^{n-1}\}$ и называть *множеством критерия распространения* для функции f. Мощность этого множества обозначим через pc_f. Очевидно, что $0 \leqslant pc_f \leqslant 2^n - 1$. Достижимость указанных выше границ можно продемонстрировать на примере булевых функций из известных классов. Для произвольного n и произвольной аффинной функции из $\mathcal{F}_n$ её pc_f равна 0 (так как производная аффинной функции по любому направлению является константой, см. [2]). Для чётного n и для произвольной бент-функции из $\mathcal{F}_n$ её pc_f равна $2^n - 1$ (критерий Ротхауза, см. [7]).

Напрямую из теоремы о взаимной корреляции следует утверждение, характеризующее векторы из множества $E_{PC}(f)$.

Теорема 2 ([2], [3]). *Вектор $u \in V_n$ принадлежит $E_{PC}(f)$ тогда и только тогда, когда выполнено равенство*

$$\sum_{x \in V_n} (-1)^{\langle x,u \rangle} W_f^2(x) = 0.$$

Булева функция $f \in \mathcal{F}_n$ называется ***корреляционно-иммунной порядка m***, если её преобразование Уолша–Адамара W_f удовлетворяет равенству $W_f(u) = 0$ при всех $u \in V_n$, $1 \leqslant wt(u) \leqslant m$.

Уравновешенная корреляционно-иммунная функция $f \in \mathcal{F}_n$ порядка m называется ***m-устойчивой*** функцией. Иными словами, в дополнение к предыдущему определению добавляется условие уравновешенности $W_f(0^n) = 0$. Очевидно, что если функция корреляционно-иммунна порядка m (или m-устойчива), $m > 1$, то она корреляционно-иммунна порядка j (или j-устойчива), где $1 \leqslant j < m$.

Пусть $f \in \mathcal{F}_n$. Обозначим

$$N\Delta_f = \#\{x \in V_n : \Delta_f(x) \neq 0\},$$

$$NW_f = \#SW_f = \#\{x \in V_n : W_f(x) \neq 0\}.$$

Функция $f \in \mathcal{F}_n$ называется ***частично бент-функцией***, если $N\Delta_f \cdot NW_f = 2^n$. Эквивалентное определение ([2]): функция $f \in \mathcal{F}_n$ называется частично бент-функцией, если существует такой вектор $\alpha \in V_n$, что для любого $u \in V_n$ значение $\Delta_f(u)$ равно или 0, или $(-1)^{\langle \alpha,u \rangle} 2^n$.

Функция $f \in \mathcal{F}_n$ называется ***платовидной порядка $2r$***, $0 \leqslant r \leqslant n/2$, если квадрат каждого коэффициента Уолша–Адамара равен либо 2^{2n-2r}, либо 0. Очевидно, что $NW_f = 2^{2r}$.

Теорема 3 ([2]). *Пусть $f \in \mathcal{F}_n$ — платовидная функция порядка $2r < n$. Следующие условия эквивалентны:*

1. *f — частично бент-функция,*
2. *$N\Delta_f = 2^{n-2r}$.*

III. Булевы функции с мощностью множества критерия распространения, равной $2^n - 2$

В этом разделе рассмотрим вопросы, связанные с булевыми функциями, у которых мощность множества критерия распространения pc_f равна $2^n - 2$, — существуют ли такие функции при любом натуральном n и принадлежат ли они к какому-нибудь криптографическому классу. Кроме того, покажем связь между множеством булевых функций, обладающих таким свойством, и множеством бент-функций.

A. Существование функций

Для рассмотрения вопроса существования функций, у которых мощность множества критерия распространения pc_f равна $2^n - 2$, нам потребуется следующее арифметическое утверждение.

Лемма 1. *Пусть n — натуральное число, $n \geqslant 2$ и p, q, c $(c \neq 0)$ — целые числа такие, что выполнена система уравнений*

$$\begin{cases} 2^n + c = p^2; \\ 2^n - c = q^2. \end{cases} \tag{1}$$

Тогда n — нечётное, и система (1) имеет четыре решения:

1. $c = 2^n,\ p = 2^{\frac{n+1}{2}},\ q = 0;$
2. $c = 2^n,\ p = -2^{\frac{n+1}{2}},\ q = 0;$
3. $c = -2^n,\ p = 0,\ q = 2^{\frac{n+1}{2}};$
4. $c = -2^n,\ p = 0,\ q = -2^{\frac{n+1}{2}}.$

Доказательство. Предположим, что $q = 0$. Тогда, подставив значение q в систему (1), очевидно, что $c = 2^n$, $p = \pm 2^{\frac{n+1}{2}}$ и n действительно нечётно. Аналогичным образом при $p = 0$ получим, что n нечётно, а также $c = -2^n$ и $q = \pm 2^{\frac{n+1}{2}}$.

Теперь докажем, что больше не существует других решений системы (1). Сначала предположим, что $|p| = |q|$. Тогда решений системы (1) нет, так как в противном случае выполнялось бы равенство $c = 0$, что противоречит условию леммы. Таким образом, не умаляя общности, будем считать, что $c > 0$ и $p^2 > q^2 > 0$ (случай при $c < 0$ и $q^2 > p^2 > 0$ доказывается аналогичным образом).

Разложим числа p, q и c на простые множители и выделим наибольшие степени 2, на которые эти числа делятся, т. е. $c = 2^s\alpha$, $p = \pm 2^t\beta$, $q = \pm 2^l\gamma$, где α, β, γ — целые нечётные числа, $s, t, l \geqslant 0$. Тогда система (1) принимает вид

$$\begin{cases} 2^n = 2^{2t}\beta^2 - 2^s\alpha; \\ 2^n = 2^{2l}\gamma^2 + 2^s\alpha. \end{cases} \tag{2}$$

Рассмотрим второе уравнение системы (2). Если предположить, что $n \leqslant 2l$, то получим

$$-2^s\alpha = 2^n(2^{2l-n}\gamma^2 - 1),$$

что невозможно, поскольку в наших предположениях левая часть уравнения строго отрицательная, а правая часть уравнения неотрицательная. Таким образом, $n > 2l$. Кроме того, проведя аналогичные рассуждения, получим, что $n > s$.

Теперь предположим, что $2l < s$. Тогда

$$2^n = 2^{2l}(\gamma^2 + 2^{s-2l}\alpha) \Rightarrow 2^{n-2l} = \gamma^2 + 2^{s-2l}\alpha.$$

Поскольку $n > 2l$, то в левой части уравнения стоит чётное число. С другой стороны, так как γ^2 — нечётное и $s > 2l$, то в правой части уравнения стоит нечётное число. Получаем противоречие. Следовательно, $2l \geqslant s$.

Таким образом, второе уравнение системы (2) можно представить в следующем виде:

$$2^n = 2^s(2^{2l-s}\gamma^2 + \alpha) \Rightarrow 2^{n-s} = 2^{2l-s}\gamma^2 + \alpha.$$

Допустим, что $2l > s$. Тогда на основании того, что $n > s$ и α — нечётное, приходим к выводу, что левая часть уравнения чётная, а правая — нечётная. Получили противоречие. Значит, $2l = s$, и в результате уравнение принимает вид

$$2^{n-s} = \gamma^2 + \alpha. \tag{3}$$

Рассмотрим первое уравнение системы (2) и предположим, что $n \leqslant 2t$. Так как $n > s$, то получим

$$2^s\alpha = 2^n(2^{2t-n}\beta^2 - 1) \Rightarrow \alpha = 2^{n-s}(2^{2t-n}\beta^2 - 1).$$

Однако в левой части уравнения стоит нечётное число, а в правой части — чётное, что является противоречием. Следовательно, $n > 2t$.

Теперь предположим, что $2t < s$. Тогда

$$2^n = 2^{2t}(\beta^2 - 2^{s-2t}\alpha) \Rightarrow 2^{n-2t} = \beta^2 - 2^{s-2t}\alpha.$$

Поскольку $n > 2t$, то в левой части уравнения стоит чётное число. Однако в правой части уравнения стоит нечётное число, так как β^2 — нечётное и $2t < s$, что в итоге приводит к противоречию. Следовательно, $2t \geqslant s$.

Таким образом, первое уравнение системы (2) можно переписать в следующем виде

$$2^n = 2^s(2^{2t-s}\beta^2 - \alpha) \Rightarrow 2^{n-s} = 2^{2t-s}\beta^2 - \alpha.$$

Допустим, что $2t > s$. Так как $n > s$ и α — нечётное, то отсюда заключаем, что левая часть уравнения чётная, а правая — нечётная. Получили противоречие. Следовательно, $2t = s$, и в результате первое уравнение системы (2) принимает вид

$$2^{n-s} = \beta^2 - \alpha. \tag{4}$$

Объединив уравнения (3) и (4), получим соотношение

$$\beta^2 - \alpha = \gamma^2 + \alpha \Rightarrow \beta^2 - \gamma^2 = (\beta - \gamma)(\beta + \gamma) = 2\alpha.$$

Заметим, что левая часть уравнения кратна 4 (так как значения в обеих скобках являются чётными числами), а правая часть кратна 2, что в конце концов приводит к противоречию. Значит, система (1) при $c > 0$ и $p^2 > q^2 > 0$ не имеет решений. Лемма доказана. □

Теорема 4. *Булева функция $f \in \mathcal{F}_n$ $(n \geqslant 2)$ имеет $pc_f = 2^n - 2$ тогда и только тогда, когда n нечётно и функция f является одновременно платовидной функцией порядка $n-1$ и частично бент-функцией.*

Доказательство. Докажем достаточность условий теоремы. Из определения платовидной функции порядка $n-1$ получим, что квадрат ненулевых коэффициентов Уолша равен 2^{n+1} и, следовательно, n нечётно. Согласно теореме 3, получим $N\Delta_f = 2$ и $pc_f = 2^n - 2$.

Докажем необходимость условий теоремы. Пусть $f \in \mathcal{F}_n$ — булева функция, $n \geqslant 2$, и её $pc_f = 2^n - 2$. Тогда существуют ненулевой вектор $\alpha \in V_n$ и целое число c, $0 < |c| \leqslant 2^n$, что значения автокорреляционной функции выглядят следующим образом:

$$\Delta_f(u) = \begin{cases} 2^n, & u = 0^n; \\ c, & u = \alpha; \\ 0, & u \neq 0^n, \alpha. \end{cases}$$

По теореме о взаимной корреляции и определению матрицы Адамара–Сильвестра

$$\left(W_f^2(0^n), \ldots, W_f^2(1^n)\right) = \left(\Delta_f(0^n), \ldots, \Delta_f(1^n)\right) H_n =$$

$$= \left(\sum_{x \in V_n} (-1)^{\langle x, 0^n \rangle} \Delta_f(x), \ldots, \sum_{x \in V_n} (-1)^{\langle x, 1^n \rangle} \Delta_f(x)\right) =$$

$$= \left(2^n + (-1)^{\langle \alpha, 0^n \rangle} c, \ldots, 2^n + (-1)^{\langle \alpha, 1^n \rangle} c\right). \tag{5}$$

Таким образом, спектр Уолша булевой функции f принимает не более четырёх различных значений, и, следовательно, существуют такие целые числа p и q, что набор (c, p, q) является решением системы уравнений (1). Тогда, согласно лемме 1, n нечётно, и система уравнений (1) имеет следующие четыре решения:

1. $c = 2^n,\ p = 2^{\frac{n+1}{2}},\ q = 0;$
2. $c = 2^n,\ p = -2^{\frac{n+1}{2}},\ q = 0;$
3. $c = -2^n,\ p = 0,\ q = 2^{\frac{n+1}{2}};$
4. $c = -2^n,\ p = 0,\ q = -2^{\frac{n+1}{2}}.$

Воспользовавшись определениями частично бент-функции и платовидной функции порядка $n-1$, непосредственной проверкой несложно убедиться в необходимости условий теоремы. □

Предложение 1. *При нечётном n число $2^n - 2$ является максимально возможной величиной для мощности множества критерия распространения булевых функций из $\mathcal{F}_n$.*

Доказательство. Пусть n — нечётное. Предположим, что существует такая функция $f \in \mathcal{F}_n$, что $pc_f = 2^n - 1$. Тогда по теореме о взаимной корреляции

$$W_f^2(u) = \sum_{x \in V_n} (-1)^{\langle u, x \rangle} \Delta_f(x) = 2^n$$

при любом $u \in V_n$ и, следовательно, $W_f(u) = \pm 2^{\frac{n-1}{2}}\sqrt{2}$. Однако преобразование Уолша–Адамара является целочисленной функцией, что приводит к противоречию. Значит, при нечётном n не существует булевой функции $f \in \mathcal{F}_n$ с $pc_f = 2^n - 1$. □

Непосредственно из теоремы 4 вытекают очевидные утверждения.

Следствие 2. *Нелинейность $nl(f)$ булевой функции $f \in \mathcal{F}_n$, $pc_f = 2^n - 2$, равна $2^{\frac{n-1}{2}}(2^{\frac{n-1}{2}} - 1)$.*

Следствие 3. *Булева функция $f \in \mathcal{F}_n$, $pc_f = 2^n - 2$, является уравновешенной тогда и только тогда, когда $\Delta_f(\alpha) = -2^n$, где $\alpha \in V_n,\ \alpha \neq 0^n$.*

Замечание. В случае, если функция $f \in \mathcal{F}_n$, $pc_f = 2^n - 2$, не является уравновешенной, то на основе функции f можно построить уравновешенную функцию, сохранив нелинейность и мощность множества критерия распространения (см. [1] и [4]). Для этого достаточно выбрать ненулевой вектор $\omega \in V_n$ такой, что $W_f(\omega) = 0$, и преобразовать функцию f в функцию $f^*(x) = f(x) \oplus \oplus \langle x, \omega \rangle$. Нетрудно убедиться, что функция f^* является уравновешенной.

Пример 1. Пусть $f \in \mathcal{F}_3$, $f(x_1, x_2, x_3) = x_2 \oplus x_2x_3 \oplus \oplus x_1x_3 \oplus x_1x_2$. Тогда её значения спектра Уолша W_f и автокорреляционной функции Δ_f имеют следующий вид:

x_1	x_2	x_3	$f(x_1, x_2, x_3)$	W_f	Δ_f
0	0	0	0	4	8
0	0	1	0	0	0
0	1	0	1	0	0
0	1	1	0	4	0
1	0	0	0	0	0
1	0	1	1	-4	0
1	1	0	0	4	0
1	1	1	0	0	8

Таблица 1. Спектр Уолша и автокорреляционная функция булевой функции f.

Из таблицы видно, что булева функция f является частично бент-функцией и платовидной функцией порядка 2, её нелинейность $nl(f)$ равна 2, а её мощность множества критерия распространения pc_f равна 6.

B. Связь между множеством функций из $\mathcal{F}_n$, $pc_f = 2^n - 2$, и множеством бент-функций $\mathcal{B}_{n-1}$

Приведём без доказательства следующее утверждение.

Предложение 2 ([5]). *Пусть $C \subseteq V_n$ — аффинное подпространство размерности k (k чётно). Тогда существует взаимно однозначное соотношение между множеством платовидных функций $f \in \mathcal{F}_n$, у которых носитель спектра Уолша SW_f совпадает с C, и множеством бент-функций $\mathcal{B}_k$. Кроме того, все ненулевые коэффициенты Уолша–Адамара W_f функции f равны по модулю $2^{n-k/2}$.*

Справедлива следующая характеризация булевых функций, у которых мощность множества критерия распространения равна $2^n - 2$.

Теорема 5. *Существует взаимно однозначное соотношение между множеством функций $f \in \mathcal{F}_n$, $pc_f = 2^n - 2$, и множеством бент-функций $\mathcal{B}_{n-1}$. Более того, количество всех булевых функций, у которых $pc_f = 2^n - 2$, равно $2(2^n - 1) \cdot \#\mathcal{B}_{n-1}$.*

Доказательство. Поскольку $pc_f = 2^n - 2$, то существуют вектор $\alpha \in V_n \neq 0^n$ и целое число c, $0 < |c| \leqslant 2^n$, такие, что $\Delta_f(\alpha) = c \neq 0$. Из теоремы 4 ясно, что n нечётно, $c \in \{2^n, -2^n\}$, а функции f, $pc_f = 2^n - 2$, являются платовидными функциями порядка $n-1$. Кроме того, согласно тождеству (5), носитель спектра Уолша SW_f имеет вид

$$SW_f = \{u \in V_n \colon \langle \alpha, u \rangle = \lambda\}, \text{ где } \lambda = \begin{cases} 0, & c = 2^n, \\ 1, & c = -2^n. \end{cases}$$

Нетрудно понять, что множество SW_f является аффинным подпространством V_n и имеет размерность $n-1$. Тогда по предложению 2 существует взаимно однозначное соотношение между множеством функций f, $pc_f = 2^n - 2$, и множеством бент-функций $\mathcal{B}_{n-1}$. Более того, исходя из взаимной однозначности, видно, что количество функций f, обладающих $pc_f = 2^n - 2$ и имеющих один и тот же носитель спектра SW_f, равно мощности множества $\mathcal{B}_{n-1}$.

С другой стороны, носитель спектра Уолша SW_f зависит только от вектора α и значения $c \in \{2^n, -2^n\}$. Следовательно, количество всех возможных носителей спектра Уолша равно $2(2^n - 1)$. Перемножив оба полученных значения, получим утверждение теоремы. □

В заключение этого раздела отметим следующие конструкции булевых функций, основанные на частных случаях взаимно однозначного соответствия, описанного в предложении 2.

Предложение 3 ([8]). *Пусть n нечётно. Введём булеву функцию $f \in \mathcal{F}_n$, которая задаётся равенством*

$$f(x_1, \ldots, x_n) = x_1 \oplus g(x_1 \oplus x_2, \ldots, x_1 \oplus x_n),$$

где $g \in \mathcal{F}_{n-1}$ — бент-функция. Тогда функция f является уравновешенной функцией, удовлетворяющей критерию распространения по всем направлениям из V_n, кроме $\omega^* = 1^n$.

Предложение 4 ([9]). *Пусть n нечётно. Введём булеву функцию $f \in \mathcal{F}_n$, которая задаётся равенством*

$$f(x_1, \ldots, x_n) = g(x_1 \oplus x_n, \ldots, x_{n-1} \oplus x_n) \oplus h(x_1, \ldots, x_n),$$

где $g \in \mathcal{F}_{n-1}$ — бент-функция и $h \in \mathcal{F}_n$ — аффинная функция. Тогда функция f удовлетворяет критерию распространения по всем направлениям из V_n, кроме $\omega^* = 1^n$.

IV. Корреляционно-иммунные и устойчивые функции с $pc_f = 2^n - 2$

Теперь рассмотрим вопрос — могут ли булевы функции с $pc_f = 2^n - 2$ быть корреляционно-иммунными или устойчивыми функциями. Такие классы булевых функций представляют с точки зрения криптографических приложений определённый интерес, поскольку они способны противостоять корреляционным методам криптоанализа.

Допустим, что $f \in \mathcal{F}_n$ — m-устойчивая функция ($1 \leqslant m < n$), $pc_f = 2^n - 2$ (т. е. существует $\alpha \in V_n, \alpha \neq 0^n \colon \Delta_f(\alpha) = c \neq 0$). Тогда f является уравновешенной функцией, а также $W_f(u) = 0$, $0 \leqslant wt(u) \leqslant m$. Согласно следствию 3, получим $c = -2^n$.

С другой стороны, по теореме о взаимной корреляции, при любом $u \in V_n \colon 1 \leqslant wt(u) \leqslant m$ справедливы соотношения

$$W_f^2(u) = \sum_{x \in V_n} (-1)^{\langle x,u \rangle} \Delta_f(x) = 2^n + (-1)^{\langle \alpha,u \rangle}(-2^n) = 0 \Rightarrow$$

$$\Rightarrow \langle \alpha, u \rangle = 0,$$

что невозможно ни при каком ненулевом α. Следовательно, функция f не может быть m-устойчивой.

Теперь предположим, что $f \in \mathcal{F}_n$ — неуравновешенная корреляционно-иммунная функция порядка m ($1 \leqslant m < n$), $pc_f = 2^n - 2$ (т. е. существует $\alpha \in V_n, \alpha \neq 0^n \colon \Delta_f(\alpha) = c \neq 0$). По определению корреляционно-иммунной функции $W_f(u) = 0$, $1 \leqslant wt(u) \leqslant m$ и $W_f(0^n) \neq 0$. Иными словами, все векторы $u \in V_n$, $1 \leqslant wt(u) \leqslant m$ принадлежат множеству $\overline{SW_f} = V_n \setminus SW_f$, которое, как и SW_f, является аффинным подпространством размерности $n-1$.

Рассмотрим множество $M = \{u \in V_n \colon wt(u) = 1\}$. Поскольку набор, состоящий из всех векторов из M, является линейно независимым, а размерность $\overline{SW_f}$ равно $n-1$, то $\overline{SW_f}$ не может быть линейным подпространством. Следовательно, носитель спектра SW_f является линейным подпространством, имеющее вид $SW_f = \{u \in V_n \colon \langle \alpha, u \rangle = 0\}$, а также $c = 2^n$.

Возьмём произвольный вектор из M и прибавим его ко всем векторам из M. Полученный набор состоит из нулевого вектора и $n-1$ векторов веса 2, а также принадлежит SW_f (так как, по определению аффинного подпространства, $SW_f = u' \oplus \overline{SW_f}$, где $u' \in \overline{SW_f}$). Суммируя друг с другом векторы из этого набора, приходим к выводу, что SW_f состоит только из векторов чётного веса. Следовательно, функция f, у которой $pc_f = 2^n - 2$, является корреляционно-иммунной функцией порядка 1 тогда и только тогда, когда носитель спектра Уолша SW_f состоит только из векторов чётного веса. Кроме того, очевидно, что функция f не может быть корреляционно-иммунной порядка большего, чем 1, а

также, согласно теореме 5, количество всех булевых функций из $\mathcal{F}_n$, которые имеют $pc_f = 2^n - 2$ и являются корреляционно-иммунными функциями порядка 1, равно $\#\mathcal{B}_{n-1}$.

Таким образом, приходим к следующему утверждению:

Теорема 6.

1. *Не существует ни одной m-устойчивой булевой функции $f \in \mathcal{F}_n$, имеющей $pc_f = 2^n - 2$.*
2. *Булева функция $f \in \mathcal{F}_n$, $pc_f = 2^n - 2$, является корреляционно-иммунной функцией порядка 1 тогда и только тогда, когда её носитель спектра Уолша SW_f состоит только из векторов чётного веса. Количество всех булевых функций из $\mathcal{F}_n$, которые имеют $pc_f = 2^n - 2$ и являются корреляционно-иммунными функциями порядка 1, равно $\#\mathcal{B}_{n-1}$.*

V. Заключение

Исходя из полученных результатов, видно, что множество критерия распространения, состоящее из всех векторов n-мерного булева пространства, кроме нулевого вектора и одного некоторого ненулевого вектора, однозначно определяет вид булевых функций. Булевы функции, обладающие таким свойством, являются одновременно частично бент-функциями и платовидными функциями порядка $n-1$, могут быть уравновешенными функциями и корреляционно-иммунными функциями порядка 1, но при этом не могут быть устойчивыми функциями. Более того, показано, что существует взаимно однозначная связь между такими функциями и бент-функциями от $n-1$ переменной, и на основе этого факта определено их точное количество. В итоге, булевы функции такого типа демонстрируют свою перспективность практического применения в криптографических приложениях.

Автор выражает благодарность Ю. В. Таранникову за ценные замечания, способствовавшие улучшению изложения результатов данной работы.

Библиография

[1] Г.А. Исаев. «Критерии распространения различных классов булевых функций и их свойства» International Journal of Open Information Technologies, том 9, № 5, 2021, с. 18–24.

[2] О.А. Логачев, А.А. Сальников, С.В. Смышляев, В.В. Ященко. «Булевы функции в теории кодирования и криптологии» М.: МЦНМО, 2012, сс. 583.

[3] C. Carlet. «Boolean Functions for Cryptography and Coding Theory» Cambridge University Press, Cambridge, 2020, pp. 562.

[4] E. Pasalic, T. Johansson. «Further Results on the Relation Between Nonlinearity and Resiliency for Boolean Functions» 7th IMA International Conference on Cryptography and Coding, LNCS 1746, 1999, p. 35–44.

[5] V.N. Potapov, A.A. Taranenko, Yu.V. Tarannikov. «Asymptotic bounds on numbers of bent functions and partitions of the Boolean hypercube into linear and affine subspaces» arXiv:2108.00232 [math.CO], 2021, pp. 10.

[6] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, J. Vandewalle. «Propagation characteristics of Boolean functions» EUROCRYPT'90, LNCS 473, Springer-Verlag, 1990, p. 161–173.

[7] O.S. Rothaus. «On «Bent» Functions» Journal of Combinatorial Theory (A), V. 20, No. 3, 1976, p. 300–305.

[8] J. Seberry, X.M. Zhang, Y. Zheng. «Nonlinearly Balanced Boolean Functions and Their Propagation Characteristics» CRYPTO'93, 13th Annual International Cryptology Conference, Santa Barbara, California, USA, 1993, p. 49–60.

[9] Y. Zheng, X.M. Zhang. «On Relationships among Avalanche, Nonlinearity, and Correlation Immunity» ASIACRYPT 2000, 6th International Conference on the Theory and Application of Cryptology and Information Security, LNCS 1976, 2000, p. 470–482.

On Boolean Functions with cardinality of propagation criteria equal to $2^n - 2$

G.A. Isaev

***Abstract*—The study of the propagation criterion for Boolean functions and its properties is one of the most important areas of research in the field of cryptographic applications. Boolean function satisfies the propagation criterion to the direction (defined by a vector from the corresponding n-dimensional Boolean space) if the derivative of function in this direction is balanced. The set of all such directions (or vectors) for Boolean function is called the set of the propagation criterion.**

Note that for some classes of Boolean functions, the propagation criterion determines their extreme properties. For example, the propagation criterion of bent functions determines their maximum nonlinearity.

In this paper we consider the question of the existence of Boolean functions, which are close enough to bent functions from the point of view of the propagation criterion, i. e. such class of Boolean functions, where all vectors, except for the zero and one non-zero vector, satisfy the propagation criterion. We show that a set of Boolean functions with such property exists only for an odd number of variables. In addition, we study the question of belonging a set of Boolean functions with this property to any cryptographic classes, including correlation-immune and resilient functions, and reveal a one-to-one correspondence between these functions and bent functions.

***Keywords*—Boolean function, propagation criterion, correlation-immune function, resilient function, Walsh spectrum, autocorrelation.**

References

[1] G.A. Isaev. «On Propagation Criteria of Some Classes of Boolean Functions» International Journal of Open Information Technologies, V. 9, No. 5, 2021, p. 18–24 [in Russian].

[2] O.A. Logachev, A.A. Salnikov, S.V. Smyshlyaev, V.V. Yashchenko. «Boolean Functions in Coding Theory and Cryptography» Moscow, URSS, 2015, pp. 583 [in Russian].

[3] C. Carlet. «Boolean Functions for Cryptography and Coding Theory» Cambridge University Press, Cambridge, 2020, pp. 562.

[4] E. Pasalic, T. Johansson. «Further Results on the Relation Between Nonlinearity and Resiliency for Boolean Functions» 7th IMA International Conference on Cryptography and Coding, LNCS 1746, 1999, p. 35–44.

[5] V.N. Potapov, A.A. Taranenko, Yu.V. Tarannikov. «Asymptotic bounds on numbers of bent functions and partitions of the Boolean hypercube into linear and affine subspaces» arXiv:2108.00232 [math.CO], 2021, pp. 10.

[6] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, J. Vandewalle. «Propagation characteristics of Boolean functions» EUROCRYPT'90, LNCS 473, Springer-Verlag, 1990, p. 161–173.

[7] O.S. Rothaus. «On «Bent» Functions» Journal of Combinatorial Theory (A), V. 20, No. 3, 1976, p. 300–305.

[8] J. Seberry, X.M. Zhang, Y. Zheng. «Nonlinearly Balanced Boolean Functions and Their Propagation Characteristics» CRYPTO'93, 13th Annual International Cryptology Conference, Santa Barbara, California, USA, 1993, p. 49–60.

[9] Y. Zheng, X.M. Zhang. «On Relationships among Avalanche, Nonlinearity, and Correlation Immunity» ASIACRYPT 2000, 6th International Conference on the Theory and Application of Cryptology and Information Security, LNCS 1976, 2000, p. 470–482.