Критерии распространения различных классов булевых функций и их свойства

Г.А. Исаев

***Аннотация*—Впервые определение критерия распространения булевых функций было введено Бартом Пренеелем и соавторами в работе [5]. Это понятие представляет собой множество векторов, для которых соответствующие им производные булевой функции являются уравновешенными функциями. Оно характеризует статистические свойства семейства производных булевой функции, играющих важную роль в анализе и синтезе криптосистем.**

Для некоторых классов булевых функций критерий распространения определяет их экстремальные свойства. Например, для бент-функций критерий распространения определяет их максимальную нелинейность. Однако главным недостатком бент-функций является отсутствие уравновешенности, что означает, что такие функции не имеют равномерного распределения выходных данных. Построение уравновешенных булевых функций, обладающих высокой нелинейностью и большим числом векторов, удовлетворяющих критерию распространения, до сих пор остаётся открытой проблемой в криптографии.

В работе получены точные значения и оценки количества векторов, удовлетворяющих критерию распространения булевых функций из известных криптографических классов, таких как платовидные функции, функции из класса Майорана–МакФарланда, квадратичные функции, алгебраически вырожденные функции и мультиаффинные функции. Показано также, что число векторов, удовлетворяющих критерию распространения, является инвариантом для расширения полной аффинной группы первой степени.

***Ключевые слова*—булева функция, критерий распространения, полная аффинная группа, расширение полной аффинной группы.**

I. Введение

Среди основных криптографических свойств булевых функций большое внимание уделяется строгому лавинному критерию ([12]). Это понятие является частным случаем другого важного понятия, именуемого критерием распространения (под критерием распространения булевой функции понимают множество векторов, для которых соответствующие им производные булевой функции являются уравновешенными функциями (см. [5])). Число векторов, удовлетворяющих критерию распространения, является параметром, описывающим статистические свойства производных булевой функции. Максимальное значение этого параметра имеет место лишь при чётном числе переменных и для экстремального класса булевых функций, называемых бент-функциями, а минимальное значение достигается только у аффинных функций.

В данной работе получены точные значения и оценки количества векторов, удовлетворяющих критерию распространения булевых функций из известных криптографических классов, таких как платовидные функции, функции из класса Майорана–МакФарланда, квадратичные функции, алгебраически вырожденные функции и мультиаффинные функции. Показано также, что число векторов, удовлетворяющих критерию распространения булевой функции, является инвариантом для расширения полной аффинной группы первой степени.

Статья получена 28 декабря 2020 г.

Исаев Г.А. — МГУ им. М.В. Ломоносова (e-mail: gleb-isaev52@yandex.ru).

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 будем часто опускать знак «$\cdot$»: $ab = a \cdot b$).

Произвольную булеву функцию f из $\mathcal{F}_n$ можно представить (см. [1]) в форме полинома от n переменных, то есть

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

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

где $a_{i_1 \dots i_j} \in \mathbb{F}_2$, $j = 1, 2, \dots, n$. Такой представление функции называется ***полиномом Жегалкина*** или ***алгебраической нормальной формой (АНФ)***. Выражение $x_{i_1} \dots x_{i_j}$, $j = 1, 2, \dots, n$ (когда $a_{i_1 \dots i_j} = 1$) 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*.

Пусть $\langle a,b\rangle = a_1b_1 \oplus \cdots \oplus a_nb_n$ — скалярное прозведение векторов $a, b \in V_n$. ***Преобразованием Уолша–Адамара*** булевой функции f из $\mathcal{F}_n$ ([1]) называют целочисленную функцию W_f, задаваемую на множестве V_n равенством

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

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

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

где решётка «#» — 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 $\mathcal{A}_n \subset \mathcal{F}_n$:

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

Обычно для вычисления этого параметра пользуются соотношением:

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

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

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

Утверждение 1 ([1]). *Производная булевой функции обладает следующими легко проверяемыми свойствами:*

1. *Для любых $u, v, x \in V_n$ справедливо равенство $D_{u\oplus v}f(x) = D_uf(x) \oplus D_vf(x \oplus u)$;*
2. *Для любых $f, g \in \mathcal{F}_n$ и любого вектора $u \in V_n$ выполнено равенство $D_u(f \oplus g)(x) = D_uf(x) \oplus D_ug(x)$;*
3. *Производная функции $f \in \mathcal{F}_n$ по направлению единичного вектора $e^{(i)} \in V_n$ с единицей в i-й позиции и нулями в остальных является константой тогда и только тогда, когда функция может быть представлена в виде*

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

где $\varepsilon \in \{0,1\}$ — константа;

4. *Производная функции $f \in \mathcal{F}_n$ постоянна по каждому направлению тогда и только тогда, когда эта функция является аффинной.*

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

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

Для любой функции $f \in \mathcal{F}_n$ выполняется

$$\sum_{u \in V_n} \Delta_f(u) = W_f^2(0^n), 0^n = (\underbrace{0, \ldots, 0}_{n}).$$

Бент-функцией называется такая булева функция от n переменных, где n четно, что модуль каждого коэффициента Уолша-Адамара этой функции равен $2^{\frac{n}{2}}$.

III. Критерий распространения булевых функций

Впервые определение критерия распространения булевых функций было введено Бартом Пренеелем и соавторами в работе [5]. Это понятие характеризует статистические свойства семейства производных булевой функции, играющих важную роль в синтезе и анализе криптосистем — в частности, в хэш-функциях и блочных шифрах.

Пусть $f \in \mathcal{F}_n$ и $u \in V_n$. Булева функция f удовлетворяет ***критерию распространения*** по направлению u, если производная D_uf — уравновешенная функция (что эквивалентно условию $\Delta_f(u) = 0$). Множество всех таких векторов будем обозначать через $E_{PC}(f) = \{u \in V_n : wt(D_uf) = 2^{n-1}\}$ и называть *множеством критерия распространения* 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 (по четвёртому пункту Утверждения 1). Для чётного n и для произвольной бент-функции из $\mathcal{F}_n$ её pc_f равна $2^n - 1$ (критерий Ротхауза, см. [9]).

Ниже приводятся результаты, отражающие связи критерия распространения со спектральными и метрическими свойствами булевых функций.

Характеризация векторов из множества $E_{PC}(f)$ задаётся следующим утверждением.

Теорема 1 ([1]). *Вектор $u \in V_n$ принадлежит $E_{PC}(f)$ тогда и только тогда, когда выполнено равенство*

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

Соотношение между числом векторов критерия распространения функции, её алгебраической степенью и максимальным значением модуля коэффициентов Уолша–Адамара описывает следующее неравенство.

Утверждение 2 ([6]). *Пусть функция $f \in \mathcal{F}_n$ и имеет степень d, $d > 1$. Тогда справедливо неравенство*

$$pc_f \geqslant 2^n - 1 - 2^{n-4-2\lfloor \frac{n-2}{d-1} \rfloor}(W_{max}^2 - 2^n).$$

Булева функция $f \in \mathcal{F}_n$ удовлетворяет ***критерию распространения степени*** k (обозначение PC(k)), если $wt(D_uf) = 2^{n-1}$ для любых $u \in V_n$ таких, что $1 \leqslant wt(u) \leqslant k$.

Теорема 2 ([8]). *Пусть $f \in \mathcal{F}_n$, удовлетворяющая PC(k). Тогда*

1. $nl(f) \geqslant 2^{n-1} - 2^{n-1-\frac{1}{2}k}$;
2. *Неравенство в п. 1 обращается в равенство тогда и только тогда, когда выполняется одно из следующих условий:*
   (a) *$k = n-1$, n нечётно и $f(x)$ представима в виде $g(x_1 \oplus x_n, \ldots, x_{n-1} \oplus x_n) \oplus h(x_1, \ldots, x_n)$, где $x = (x_1, \ldots, x_n) \in V_n$, g — бент-функция из $\mathcal{F}_{n-1}$ и h — аффинная функция из $\mathcal{F}_n$;*
   (b) *$k = n$, n чётно и f — бент-функция из $\mathcal{F}_n$.*

IV. Инвариантность числа векторов, удовлетворяющих критерию распространения, относительно расширения полной аффинной группы первой степени

Напомним некоторые необходимые понятия из теории групп.

Полная аффинная группа $GA(n,2)$ **([1])** состоит из подстановок π, действие которых на V_n задаётся соотношением

$$\pi x = Ax \oplus b,$$

где $x \in V_n$, A — невырожденная $(n \times n)$-матрица с элементами из $\mathbb{F}_2$ и $b \in V_n$.

Расширение полной аффинной группы первой степени будем обозначать через $AGA_1(n,2)$ ([1]). Элементами этой группы являются пары (π, h), где $\pi \in GA(n,2)$, h — аффинная функция из $\mathcal{F}_n$.

Элемент (π, h) из группы $AGA_1(n,2)$ действует на множестве $\mathcal{F}_n$ следующим образом:

$$f^{(\pi,h)}(x) = f(\pi x) \oplus h(x), \text{ где } f \in \mathcal{F}_n.$$

Легко проверить, что такое преобразование является взаимно однозначным отображением на множестве булевых функций.

Две булевы функции f и g из $\mathcal{F}_n$ называются $AGA_1(n,2)$-***эквивалентными***, если существует преобразование $(\pi, h) \in AGA_1(n,2)$ такое, что $f^{(\pi,h)} = g$.

Справедливо следующее утверждение:

Теорема 3. *Для $AGA_1(n,2)$-эквивалентных функций f и g из $\mathcal{F}_n$ справедливо равенство*

$$pc_f = pc_g.$$

Доказательство. Так как f и g — $AGA_1(n,2)$-эквивалентные функции, то существует некоторое преобразование (ξ, h), что

$$g(x) = f^{(\xi,h)}(x) = f(Ax \oplus b) \oplus h(x),$$

где $A = (a_{ij})$ — обратимая $(n \times n)$-матрица, $a_{ij} \in \mathbb{F}_2$, $i, j = 1, 2, \ldots, n$, $b = (b_1, \ldots, b_n)^\top \in V_n$ и $h(x) \in \mathcal{F}_n$, $\deg h \leqslant 1$. Пусть $M = \{A^{-1}u : u \in E_{PC}(f)\}$. Тогда в силу обратимости матрицы A следует, что

$$\#M = \#E_{PC}(f) = pc_f.$$

Выберем произвольный ненулевой вектор $v \in M$ и рассмотрим производную

$$D_v g(x) = g(x) \oplus g(x \oplus v) = f^{(\xi,h)}(x) \oplus f^{(\xi,h)}(x \oplus v) =$$

$$= f(Ax \oplus b) \oplus h(x) \oplus f(A(x \oplus v) \oplus b) \oplus h(x) =$$

$$= f(Ax \oplus b) \oplus f(Ax \oplus b \oplus Av) = f(Ax \oplus b) \oplus f(Ax \oplus b \oplus A(A^{-1}u))$$

для некоторого $u \in E_{PC}(f)$. Введём новую переменную $y = Ax \oplus b = \xi x$. Тогда

$$D_v g(\xi^{-1} y) = f(y) \oplus f(y \oplus u) = D_u f(y)$$

Следовательно,

$$wt(D_v g) = wt(D_u f) = 2^{n-1}.$$

Таким образом, из-за взаимной однозначности преобразования (ξ, h) и, в частности, из-за обратимости матрицы A для любого ненулевого вектора $v \in M$ найдётся вектор $u \in E_{PC}(f)$, что $wt(D_v g) = wt(D_u f)$. Следовательно, $pc_g \geqslant pc_f$. Проведя аналогичные рассуждения для преобразования (ξ^{-1}, h'), при котором $f = g^{(\xi^{-1},h')}$, получаем $pc_g \leqslant pc_f$. Теорема доказана. □

V. Критерий распространения квадратичных функций

Булева функция $f \in \mathcal{F}_n$ называется ***квадратичной***, если её АНФ имеет следующий вид:

$$f(x) = f(x_1, x_2, \ldots, x_n) = \bigoplus_{1 \leqslant i < j \leqslant n} a_{ij} x_i x_j \oplus \bigoplus_{l=1}^{n} a_l x_l \oplus a_0,$$

где a_{ij} $(1 \leqslant i < j \leqslant n)$, a_l $(1 \leqslant l \leqslant n)$, a_0 — элементы поля $\mathbb{F}_2$. Полином квадратичной функции f может быть записан в следующем виде:

$$f(x) = f(x_1, x_2, \ldots, x_n) = x^\top Q_f x \oplus a_f^\top x \oplus a_0,$$

где

$$Q_f = \begin{pmatrix} 0 & a_{1,2} & a_{1,3} & \ldots & a_{1,n} \\ 0 & 0 & a_{2,3} & \ldots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & \ldots & 0 & a_{n-1,n} \\ 0 & \ldots & \ldots & \ldots & 0 \end{pmatrix}$$

— верхнетреугольная $(n \times n)$-матрица с нулевой главной диагональю, $a_f^\top = (a_1, a_2, \ldots, a_n)$. С матрицей Q_f связана следующая симметрическая матрица с нулевой главной диагональю:

$$\widetilde{Q_f} = Q_f \oplus Q_f^\top.$$

Такая матрица называется ***симплектической***. Отметим, что ранг симплектической матрицы *чётен* ([1]).

Квадратичные функции могут быть преобразованы в каноническую форму при помощи теоремы Диксона.

Теорема 4 (Диксон [11]). *Пусть $f \in \mathcal{F}_n$ — квадратичная функция, $\widetilde{Q_f}$ — её симплектическая матрица ранга r ($rank\,\widetilde{Q_f} = r$). Тогда существует такое преобразование $\xi \in GA(n,2)$, что функция f может быть приведена к одному из перечисленных ниже видов:*

1. *Если $rank\,\widetilde{Q_f} = 0$, то либо $f(\xi x) = \varepsilon$, $\varepsilon = 0, 1$, либо $f(\xi x) = x_1$;*
2. *Если $rank\,\widetilde{Q_f} = r$, $r \geqslant 2$ то либо $f(\xi x) = \bigoplus_{i=1}^{r/2} x_{2i-1} x_{2i} \oplus \varepsilon$, $\varepsilon = 0, 1$, либо $f(\xi x) = \bigoplus_{i=1}^{r/2} x_{2i-1} x_{2i} \oplus x_{r+1}$.*

Следующая теорема показывает, чему равно pc_f у квадратичных функций.

Теорема 5. *Пусть $f \in \mathcal{F}_n$ — квадратичная функция, ранг её симплектической матрицы равен r. Тогда $pc_f = (2^r - 1) \cdot 2^{n-r}$.*

Доказательство. По теореме Диксона существует преобразование $\xi \in GA(n,2)$ такое, что при $r = 0$ функция f может быть приведена к виду $g(x) = f(\xi x) = \varepsilon$,

где $\varepsilon = 0, 1$, или к $g(x) = f(\xi x) = x_1$. В случае $r \geqslant 2$ функция f может быть приведена к виду $g(x) = f(\xi x) = \bigoplus_{i=1}^{r/2} x_{2i-1}x_{2i} \oplus \varepsilon$, где либо $\varepsilon = 0, 1$, либо $\varepsilon = x_{r+1}$.

Из Теоремы 3 следует, что количества векторов критериев распространения функций f и g одинаковы. Таким образом, нам достаточно рассмотреть функцию g на предмет критерия распространения.

В случае $r = 0$ функция g является аффинной функцией, и, следовательно, получаем $pc_g = pc_f = 0$, что является искомым теоремы.

Рассмотрим случай при $r \geqslant 2$. По второму пункту Утверждения 1 для производной функции g по направлению u мы получаем

$$D_u g(x) = D_u(\bigoplus_{i=1}^{r/2} x_{2i-1}x_{2i} \oplus \varepsilon) =$$

$$= D_u(\bigoplus_{i=1}^{r/2} x_{2i-1}x_{2i}) \oplus D_u\varepsilon.$$

Поскольку $\bigoplus_{i=1}^{r/2} x_{2i-1}x_{2i}$ — бент-функция ([1]), то её pc_f равно $2^r - 1$. А так как ε является аффинной функцией, то по четвёртому пункту Утверждения 1 $D_u\varepsilon \equiv const$, и, следовательно, $x_{r+1}, \ldots, x_n$ не играют роли в критерии распространения. При фиксации переменных $x_1, \ldots, x_r$ и переборе остальных переменных получаем 2^{n-r} вариантов векторов.

Учитывая приведённые выше рассуждения, перемножаем полученные числа и получаем $pc_g = pc_f = (2^r - 1) \cdot 2^{n-r}$. Теорема доказана. □

VI. Критерий распространения алгебраически вырожденных функций

В данном разделе мы рассмотрим частный случай алгебраически вырожденных функций, а именно когда такая функция вырождается до бент-функции, и изучим его критерий распространения.

Булева функция $f \in \mathcal{F}_n$ называется ***алгебраически вырожденной***, если существуют функция $g \in \mathcal{F}_k$, $k < n$ и $(k \times n)$-матрица G ранга k ($rank\, G = k$) такие, что $f(x) = g(Gx)$.

Теорема 6. *Пусть $f \in \mathcal{F}_n$ — алгебраически вырожденная функция, $f(x) = g(Gx)$, где $g \in \mathcal{F}_k$, $k < n$, — бент-функция, G — $(k \times n)$-матрица ранга k. Введём линейное отображение $\varphi_G : V_n \to V_k$ такое, что $\varphi_G(x) = Gx$. Тогда вектор $u \in V_n$ удовлетворяет критерию распространения функции f тогда и только тогда, когда он не лежит в ядре отображения* $\ker \varphi_G = \{x \in V_n : \varphi_G(x) = 0^k\}$.

Доказательство. Рассмотрим автокорреляционную функцию булевой функции f от ненулевого вектора u:

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

$$= \sum_{x \in V_n} (-1)^{g(Gx) \oplus g(G(x \oplus u))} = \sum_{x \in V_n} (-1)^{g(Gx) \oplus g(Gx \oplus Gu)}.$$

Введём новую переменную $y \in V_k$, $y = Gx$. Так как $\dim \ker \varphi_G = n - k$, то пространство V_n раскладывается на 2^k смежных классов по ядру $\ker \varphi_G$. Тогда мы имеем

$$\sum_{x \in V_n} (-1)^{g(Gx) \oplus g(Gx \oplus Gu)} = 2^k \sum_{y \in V_k} (-1)^{g(y) \oplus g(y \oplus Gu)}.$$

Согласно определению, вектор u удовлетворяет критерию распространения, если $\Delta_f(u) = 0$. Если $u \in \ker \varphi_G$, то $\varphi_G(u) = Gu = 0$, и, следовательно, $\Delta_f(u) = 2^k \sum_{y \in V_k} (-1)^{g(y) \oplus g(y)} = 2^k \cdot 2^k = 2^{2k}$. Таким образом, вектор $u \in \ker \varphi_G$ не удовлетворяет критерию распространения.

Пусть $u \notin \ker \varphi_G$. Тогда из-за того, что функция g — бент-функция, то её производная $D_{Gu} g$ уравновешена, и поэтому $\Delta_f(u) = 0$. Значит, вектор u удовлетворяет критерию распространения. Теорема доказана. □

Следствие 1. *Пусть $f \in \mathcal{F}_n$ — алгебраически вырожденная функция, $f(x) = g(Gx)$, где $g \in \mathcal{F}_k$, $k < n$ — бент-функция, G — $(k \times n)$-матрица ранга k. Тогда $pc_f = 2^n - 2^{n-k}$.*

VII. Функции из класса Майорана–МакФарланда

Конструкция Майорана–МакФарланда используется для построения различных криптографических классов булевых функций. В связи с этим представляет интерес изучение параметров критерия распространения таких функций.

Справедливо следующее утверждение:

Теорема 7. *Пусть $n \in \mathbb{N}$, $r \in \{1, \ldots, n-1\}$, $n - r \leqslant r$, $g \in \mathcal{F}_{n-r}$, $\Phi : V_{n-r} \to V_r$, Φ — инъективное отображение. Введём булеву функцию $f : V_n = V_r \times V_{n-r} \to \mathbb{F}_2$, которая задаётся равенством*

$$f(z) = f(x, y) = \langle x, \Phi(y) \rangle \oplus g(y),$$

*где $z = (x, y) \in V_n$, $x \in V_r$, $y \in V_{n-r}$. Тогда справедливо неравенство $pc_f \geqslant (2^{n-r} - 1) \cdot 2^r$ (способ синтеза булевых функций, описанный выше, называется **конструкцией Майорана–МакФарланда** ([13])).*

Доказательство. Выберем произвольный вектор $b \in V_n$, $b = (u, v)$, $z \oplus b = (x \oplus u, y \oplus v)$ и посчитаем по его направлению производную функции f.

$$D_b f(z) = f(z \oplus b) \oplus f(z) =$$

$$= \langle x \oplus u, \Phi(y \oplus v) \rangle \oplus g(y \oplus v) \oplus \langle x, \Phi(y) \rangle \oplus g(y) =$$

$$= \langle x, \Phi(y \oplus v) \oplus \Phi(y) \rangle \oplus \langle u, \Phi(y \oplus v) \rangle \oplus g(y \oplus v) \oplus g(y).$$

Так как $n - r \leqslant r$ и отображение Φ — инъективно, то $\Phi(y \oplus v) \neq \Phi(y)$, если $wt(v) \geqslant 1$. Эта производная уравновешена, так как при фиксации y она является линейной функцией относительно вектора x. Число ненулевых векторов v равно $2^{n-r} - 1$. Поскольку этот результат не зависит от выбора вектора u, то мы получаем число всех возможных вариантов u, равное 2^r.

Учитывая приведённые выше рассуждения, перемножаем полученные числа и получаем $pc_f \geqslant (2^{n-r} - 1) \cdot 2^r$. Теорема доказана. □

VIII. Критерий распространения платовидных функций

Значительный интерес для криптографии представляют платовидные функции. Изучим применительно к этому классу критерий распространения.

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. Если мы не хотим подчёркивать конкретное значение r, то будем использовать термин *платовидная функция*.

Теперь приведём без доказательства небольшую лемму.

Лемма 1 ([1]). *Пусть f — платовидная функция порядка $2r < n$ из $\mathcal{F}_n$. Следующие условия эквивалентны:*

1. *Число ненулевых значений автокорреляционной функции $N\Delta_f$ равно 2^{n-2r};*
2. *$\dim E_f = n - 2r$ ($E_f = \{u \in V_n : D_u f \equiv const\}$ — пространство линейных структур).*

На основе этой леммы выведем следующий результат.

Лемма 2. *Пусть f — платовидная функция порядка $2r < n$ из $\mathcal{F}_n$, $\dim E_f = n - 2r$. Тогда $pc_f = 2^n - 2^{n-2r}$.*

Доказательство. Из Леммы 1 следует, что $N\Delta_f = 2^{n-2r}$. Тогда по определению критерия распространения $pc_f = 2^n - N\Delta_f = 2^n - 2^{n-2r}$. □

Теперь рассмотрим вопрос о критерии распространения подкласса платовидных функций.

Функции $g_1, g_2 \in \mathcal{F}_n$, n — нечётное, называются ***взаимно дополняющими платовидными функциями порядка*** $(n-1)$, если для любого $u \in V_n$ либо $W_{g_1}(u) = 0, W^2_{g_2}(u) = 2^{n+1}$, либо $W^2_{g_1}(u) = 2^{n+1}, W_{g_2}(u) = 0$.

Далее нам потребуется следующая теорема.

Теорема 8 ([1]). *Функции $g_1, g_2 \in \mathcal{F}_n$ являются взаимно дополняющими платовидными функциями порядка $n-1$ тогда и только тогда, когда выполнено одно из двух эквивалентных условий:*

1. *$W^2_{g_1}(u) + W^2_{g_2}(u) = 2^{n+1}$ для любого $u \in V_n$;*
2. *$\Delta_{g_1}(u) + \Delta_{g_2}(u) = 0$ для любого ненулевого $u \in V_n$.*

Из неё можно вывести следующий результат.

Теорема 9. *Пусть n — нечётное и $g_1, g_2 \in \mathcal{F}_n$ — взаимно дополняющие платовидные функции порядка $n-1$. Тогда $E_{PC}(g_1) = E_{PC}(g_2)$.*

Доказательство. По Теореме 8 имеем $\Delta_{g_1}(u) + \Delta_{g_2}(u) = 0$ для любого ненулевого $u \in V_n$. В случае, если $\Delta_{g_1}(u)$ равно 0, мы получаем, что $\Delta_{g_2}(u)$ тоже равно 0, и наоборот. Таким образом, $E_{PC}(g_1) = E_{PC}(g_2)$. Теорема доказана. □

IX. Критерий распространения мультиаффинных функций

Булева функция $f \in \mathcal{F}_n$ называется ***мультиаффинной***, если существует представление функции f в виде произведения аффинных функций:

$$f = \prod_{i=1}^{t}(a_{i1}x_1 \oplus a_{i2}x_2 \oplus \cdots \oplus a_{in}x_n \oplus a_{i0}),$$

где $a_{ij} \in \mathbb{F}_2, i = 1, \ldots, t, j = 0, \ldots, n$.

Изучим её критерий распространения. Для этого рассмотрим мультиаффинную функцию f из $\mathcal{F}_n$ и определим матрицу A и вектор A_0 следующим образом:

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{t1} & a_{t1} & \ldots & a_{tn} \end{pmatrix} = [A_1, A_2, \ldots, A_n] \text{ и } A_0 = \begin{pmatrix} a_{10} \\ a_{20} \\ \vdots \\ a_{t0} \end{pmatrix},$$

где $A_1, \ldots, A_n$ — столбцы матрицы A.

Нетрудно понять, что носитель функции $supp(f)$ представляет собой плоскость, описываемую системой линейных уравнений ([11]):

$$Ax = A_0 \oplus 1^t. \qquad (*)$$

В случае совместности системы $(*)$ число её решений равно $2^{n-rank\,A}$. Множество $supp(f)$ является смежным классом по подпространству $L = \{x \in V_n : Ax = 0^t\}$ и, кроме того, для любого $u \in L$ выполняется тождество $D_u f \equiv 0$. Тогда справедливо следующее утверждение:

Утверждение 3. *Пусть $f \in \mathcal{F}_n$ — мультиаффинная функция. Тогда $pc_f \leqslant 2^n(1 - 2^{-rank\,A})$.*

X. Заключение

В данной работе были получены точные значения и оценки количества векторов, удовлетворяющих критерию распространения известных криптографических классов булевых функций, таких как платовидные функции, функции из класса Майорана–МакФарланда, квадратичные функции, алгебраически вырожденные функции и мультиаффинные функции. Также показано, что число векторов, удовлетворяющих критерию распространения булевой функции, является инвариантом для расширения полной аффинной группы первой степени. Полученные результаты могут быть использованы в синтезе криптографических примитивов с заданными свойствами, вычислении метрических и комбинаторных параметров криптографических булевых функций, а также для расчёта параметров некоторых классов методов криптоанализа.

Библиография

[1] О.А. Логачев, А.А. Сальников., С.В. Смышляев, В.В. Ященко. «Булевы функции в теории кодирования и криптологии» М.: Московский центр непрерывного математического образования, 583 с., 2012.

[2] В.В. Ященко. «О критерии распространения для булевых функций и о бент-функциях» Пробл. передачи информ., том 33, выпуск 1, 75–86 сс., 1997.

[3] И.А. Панкратова. «Булевы функции в криптографии» Томск, Издательский Дом Томского государственного университета, 88 с., 2014.

[4] B. Preneel. «Analysis and Design of Cryptographic Hash Functions» PhD thesis, Katholiek Universiteit Leuven, 242–245 pp., 2003.

[5] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, J. Vandewalle. «Propagation characteristics of Boolean functions» Advances in Cryptology — EUROCRYPT'90, Lecture Notes in Computer Science, V. 437, Springer-Verlag, Berlin, Heidelberg, New-York, 155–165 pp., 1990.

[6] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine. «Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions» Lecture Notes in Computer Science, 1807, 16 p., 2000.

[7] J. Seberry, X.M. Zhang, Y. Zheng. «Nonlinearity and Propagation Characteristics of Balanced Boolean Functions» Crypto'93 — Advances in Cryptography, 773, Lecture Notes in Computer Science, Springer–Verlag, Berlin, 29 p., 1994.

[8] Y. Zheng, X.M. Zhang. «On Relationships among Avalanche, Nonlinearity, and Correlation Immunity» Advances in Cryptology — ASIACRYPT 2000, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 13 p., 1976 (2000).

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

[10] R.J. McEliece. «Weight congruences for p-ary cyclic codes» Discrete Mathematics, V. 3, 177–192 pp., 1972.

[11] F.J. MacWilliams, N.J.A. Sloane. «The Theory of Error-Correcting Codes» Amsterdam, New York, Oxford: North-Holland Publishing Company, 1977.

[12] A.F. Webster, S.E. Tavares. «On the design of S-boxes» Crypto'85 — Advances in Cryptology, 219, Lecture Notes in Computer Science, Springer–Verlag, 523–534 pp., 1985.

[13] R.L. McFarland. «A Family of Difference Sets in Non-cyclic Groups» Journal of Combinatorial Theory (A), V. 15, No. 1, 1–10 pp., 1973.

On Propagation Criteria of Some Classes of Boolean Functions

G.A. Isaev

***Abstract*—The definition of the propagation criterion of Boolean functions was introduced by Bart Preneel and co-authors in [5]. This concept represent a set of vectors, for which the corresponding derivatives of a Boolean function are balanced. It characterizes the statistical properties of a family of Boolean function derivatives that play an important role in the cryptosystem analysis and synthesis.**

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. However, the main disadvantage of bent functions is the lack of balancedness, which means that such functions do not have a uniform output distribution. The construction of balanced Boolean functions having a high nonlinearity and a large number of vectors satisfying the propagation criterion is still an open problem in cryptography.

In this paper we obtain exact values and estimates of the number of vectors satisfying the propagation criterion of Boolean functions from well-known cryptographic classes, such as plateaued functions, Maiorana-McFarland functions, quadratic functions, algebraic degenerate functions and multiaffine functions. We also show that the number of vectors satisfying the propagation criterion is an invariant for the extension of the general affine group of the first degree.

***Keywords*—Boolean functions, propagation criterion, general affine group, extension of the general affine group.**

References

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

[2] V.V. Yashchenko. «On Propagation Criterion of Boolean Functions and Bent-Functions» Probl. Peredachi Inf., Volume 33, Issue 1, 75–86 pp., 1997 [in Russian].

[3] I.A. Pankratova. «Boolean Functions in Cryptography» Tomsk. Gos. Univ., Tomsk, 88 p., 2014 [in Russian].

[4] B. Preneel. «Analysis and Design of Cryptographic Hash Functions» PhD thesis, Katholiek Universiteit Leuven„ 242–245 pp., 2003.

[5] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, J. Vandewalle. «Propagation characteristics of Boolean functions» Advances in Cryptology — EUROCRYPT'90, Lecture Notes in Computer Science, V. 437, Springer-Verlag, Berlin, Heidelberg, New-York, 155–165 pp., 1990.

[6] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine. «Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions» Lecture Notes in Computer Science, 1807, 16 p., 2000.

[7] J. Seberry, X.M. Zhang, Y. Zheng. «Nonlinearity and Propagation Characteristics of Balanced Boolean Functions» Crypto'93 — Advances in Cryptography, 773, Lecture Notes in Computer Science, Springer–Verlag, Berlin, 29 p., 1994.

[8] Y. Zheng, X.M. Zhang. «On Relationships among Avalanche, Nonlinearity, and Correlation Immunity» Advances in Cryptology — ASIACRYPT 2000, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 13 p., 1976 (2000).

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

[10] R.J. McEliece. «Weight congruences for p-ary cyclic codes» Discrete Mathematics, V. 3, 177–192 pp., 1972.

[11] F.J. MacWilliams, N.J.A. Sloane. «The Theory of Error-Correcting Codes» Amsterdam, New York, Oxford: North-Holland Publishing Company, 1977.

[12] A.F. Webster, S.E. Tavares. «On the design of S-boxes» Crypto'85 — Advances in Cryptology, 219, Lecture Notes in Computer Science, Springer–Verlag, 523–534 pp., 1985.

[13] R.L. McFarland. «A Family of Difference Sets in Non-cyclic Groups» Journal of Combinatorial Theory (A), V. 15, No. 1, 1–10 pp., 1973.