Некоторые свойства аффинных ограничений булевых функций и отображений

Мишанова Е. М.

***Аннотация*—Статья обобщает ряд исследований аффинных ограничений булевых функций и отображений. В работе изучаются свойства уровня и обобщенного уровня аффинности, а также их связь с параметрами, описывающими другие свойства булевых функций, даются асимптотические оценки и рассматриваются цели дальнейших работ в этой области.**

***Ключевые слова*—булевы отображения, криптография, обобщенный уровень аффинности, системы булевых уравнений, уровень аффинности.**

I. Введение

В статье рассматриваются ограничения булевых функций, совпадающие с аффинными функциями. При этом вид параметра зависит от характера области ограничения, которое он задает. Уровень аффинности характеризует эффективность одного из возможных методов линеаризации для решения систем булевых уравнений, связанного с фиксацией некоторого подмножества переменных и сведением исходной системы к линейному следствию. Вычисление обобщенного уровня аффинности основано на поиске плоскостей, ограничение функции на любую из которых совпадает с аффинной функцией. На оценку этих параметров опирается один из подходов к анализу криптографических свойств булевых отображений.

Исследования уровня аффинности направлены на развитие криптографических методов и средств обеспечения информационной безопасности. Результаты могут быть применены для выбора параметров и анализа стойкости потоковых шифров.

II. Основные определения и понятия

Обозначим через V_n n-мерное векторное пространство над полем Галуа F_2. Элементами V_n являются булевы векторы длины n. Вес Хемминга вектора $x = (x^{(1)}, x^{(2)}, \dots, x^{(n)}) \in V_n$ определяется как $wt(x) = \sum_{i=1}^{n} x_i$.

Плоскость размерности r в пространстве V_n определяется как смежный класс $\pi = L \oplus v$, где L – некоторое подпространство V_n, $\dim L = r$, и $v \in V_n$. Будем считать, что $\dim \pi = -1$, если $\pi = \emptyset$, и $\dim \pi = 0$, если $\pi = \{u\}$, $u \in V_n$. Множество всех плоскостей пространства V_n (включая пустую плоскость) обозначим через $P(V_n)$.

Статья получена 21 мая 2014. Представляет собой результат одного из этапов работы над магистерской диссертацией. Автор - магистрант факультета ВМК МГУ им. М.В. Ломоносова, e-mail: mishanovae@gmail.com

Плоскость π размерности r, $r \geq 1$, представляет собой набор решений $x = (x^{(1)}, x^{(2)}, \dots, x^{(n)})^T \in V_n$ системы линейных уравнений вида $Ax = a$, где A – $n \times n$-матрица над F_2 ранга $n - r$, и $a \in V_n$.

Специальными обозначениями выделим следующие векторы из V_n: $0 = (0, 0, \dots, 0)^T$; $1 = (1, 1, \dots, 1)^T$; $\{e_1, e_2, \dots, e_n\}$ — канонический базис V_n, $e_i = (0, \dots, 0, 1, 0, \dots, 0)$, где 1 стоит в i-ой позиции, $i = 1, 2, \dots, n$.

Для любого вектора $x = (x^{(1)}, x^{(2)}, \dots, x^{(n)})^T \in V_n$ имеем $x = x^{(1)}e_1 \oplus x^{(2)}e_2 \oplus \dots \oplus x^{(n)}e_n$, где «$\oplus$» — обозначение как сложения в F_2, так и покомпонентного сложения векторов в V_n.

Через $F_{n,m}$ обозначим множество всех отображений $V_n \to V_m$, n и m — натуральные числа. В случае $m = 1$, имеем множество $F_{n,1} = F_n$ всех отображений из V_n в F_2, то есть множество всех булевых функций от n переменных. Для булевой функции $f \in F_n$ её значение на векторе $x = x^{(1)}e_1 \oplus \dots \oplus x^{(n)}e_n$ будем обозначать $f(x) = f(x^{(1)}e_1 \oplus \dots \oplus x^{(n)}e_n) = f(x^{(1)}, \dots, x^{(n)})$.

Обозначим через $A_{n,m}$ подмножество аффинных отображений множества $F_{n,m}$.

Определение. Пусть $\Phi \in F_{n,m}$. Плоскость $\pi \in P(V_n)\backslash\{\emptyset\}$ называется *плоскостью аффинности* Φ, если $\Phi(\pi) \in P(V_m)$.

Набор $P_\Phi(V_n) = \{\pi \in P(V_n)\backslash\{\emptyset\} \mid \Phi(\pi) \in P(V_m)\backslash\{\emptyset\}\}$ - семейство плоскостей аффинности Φ. Для конкретного d, $0 \leq d \leq n$, набор $P_\Phi^d(V_n) = \{\pi \in P(V_n)\backslash\{\emptyset\} \mid \Phi(\pi) \in P(V_m), \dim \pi = d\}$ – семейство плоскостей аффинности размерности d.

Пусть $\Phi \in F_{n,m}$ и M — произвольное подмножество пространства V_n. Ограничением $\Phi|_M$ отображения Φ на множество M будем называть отображение Φ’ такое, что Φ’(x) = $\Phi|_M$ (x) = Φ (x) для всех $x \in M$.

Определение. Пусть $\Phi \in F_{n,m}$. Плоскость $\pi \in P(V_n)\backslash\{\emptyset\}$ называется *плоскостью локальной аффинности* Φ, если существует аффинное отображение $\psi = \psi(\pi) \in A_{n,m}$, такое что $\Phi|_\pi = \psi|_\pi$.

Обозначим совокупность локальных аффинностей отображения Φ как $\tilde{P}_\Phi(V_n) = \{\pi \in P(V_n)\backslash\{\emptyset\} \mid \exists \psi = \psi(\pi) \in A_{n,m} : \Phi|_\pi = \psi|_\pi\}$. Для конкретного d, $0 \leq d \leq n$, набор $\tilde{P}_\Phi^d(V_n) = \{\pi \in P(V_n)\backslash\{\emptyset\} \mid \exists \psi = \psi(\pi) \in A_{n,m} : \Phi|_\pi = \psi|_\pi, \dim \pi = d\}$ – семейство плоскостей локальной аффинности размерности d.

Для целого числа k, $0 \leq k \leq n$, набора $\{j_1, \dots, j_k\}$, $1 \leq j_1 < \dots < j_k \leq n$, и вектора $(a^{(1)}, \dots, a^{(k)}) \in V_k$ обозначим через $\pi_{j_1,\dots,j_k}^{a^{(1)},\dots,a^{(k)}}$ плоскость из $P_\Phi(V_n)$ вида

$\pi^{a^{(1)},\dots,a^{(k)}}_{j_1,\dots,j_k} = \{x \in V_n \mid x^{(j_1)} = a^{(1)}, \dots, x^{(j_k)} = a^{(k)}\}$.

Множество таких плоскостей в $\mathrm{P}_\Phi(V_n)$ обозначим как $\mathrm{Q}_\Phi(V_n)$, а $\mathrm{Q}^0_\Phi(V_n)$ – множество всех плоскостей вида $\pi^{0,\dots,0}_{j_1,\dots,j_k}$. Также обозначим $\widetilde{\mathrm{Q}}_\Phi(V_n)$ и $\widetilde{\mathrm{Q}}^0_\Phi(V_n)$ множества $\mathrm{Q}_\Phi(V_n) \cap \widetilde{\mathrm{P}}_\Phi(V_n)$ и $\mathrm{Q}^0_\Phi(V_n) \cap \widetilde{\mathrm{P}}^0_\Phi(V_n)$ соответственно.

Определение. Пусть $\Phi \in F_{n,m}$. *Уровень аффинности* отображения Φ – это неотрицательное целое $\mathrm{la}(\Phi) = \min\limits_{\pi \in \mathrm{Q}^0_\Phi(V_n)} (n - \dim \pi) = n - \max\limits_{\pi \in \mathrm{Q}^0_\Phi(V_n)} \dim \pi$. *Частичный уровень аффинности* Φ – неотрицательное целое $\mathrm{la}^0(\Phi) = \min\limits_{\pi \in \mathrm{Q}^0_\Phi(V_n)} (n - \dim \pi) = n - \max\limits_{\pi \in \mathrm{Q}^0_\Phi(V_n)} \dim \pi$.

Минимальные элементы множества $\widetilde{\mathrm{P}}_\Phi(V_n)$ – это векторы $\{\mathrm{x}\}$, $\mathrm{x} \in V_n$, являющиеся плоскостями размерности 0. Пусть $\widetilde{\mathrm{M}}_\Phi(V_n)$ – множество всех максимальных элементов $\widetilde{\mathrm{P}}_\Phi(V_n)$.

Понятие обобщенного уровня аффинности было сформулировано в [1].

Определение. Пусть $\Phi \in F_{n,m}$. *Обобщенным уровнем аффинности* отображения Φ называется неотрицательное целое $\mathrm{La}(\Phi) = \min\limits_{\pi \in \widetilde{M}_\Phi(V_n)} (n - \dim \pi) = n - \max\limits_{\pi \in \widetilde{M}_\Phi(V_n)} \dim \pi$.

Рассмотрим теперь аналогичные определения для частного случая $F_{n,m}$ при $m = 1$ – множества булевых функций. Любая функция $f \in F_n$ может быть представлена в виде двоичного вектора длины 2^n, состоящего из всех значений этой функции (порядок элементов V_n считаем фиксированным). Будем называть весом функции $\mathrm{wt}(f)$ вес соответствующего ей вектора.

Любая булева функция от *n* переменных может быть представлена в полиномиальной форме, называемой алгебраической нормальной формой (АНФ) этой функции:

$f(x) = f(x_1, \dots, x_n) = \bigoplus\limits_{u \in V_n} g(u)x^u = \bigoplus\limits_{(u_1,\dots,u_n) \in V_n} g(u_1, \dots, u_n) x_1^{u_1} \dots x_n^{u_n}$

где $g \in F_n$ и для любого $1 \le i \le n$: $x_i^{u_i} = \begin{cases} 1, & u_i = 0, \\ x_i, & u_i = 1. \end{cases}$

Алгебраической степенью $\deg(f)$ функции *f* является максимальное значение $\mathrm{wt}(u)$, для которого $g(u) \neq 0$. A_n — множество аффинных булевых функций от n переменных, то есть функций $f \in F_n$, для которых $deg(f) \le 1$.

Пусть $k \le n$, $1 \le j_1 < \dots < j_k \le n$, и вектор $(a^{(1)}, \dots, a^{(k)}) \in V_k$. Для булевой функции $f \in F_n$ обозначим через $f^{a^{(1)},\dots,a^{(k)}}_{j_1,\dots,j_k}$ булеву функцию из F_{n-k} вида $f^{a^{(1)},\dots,a^{(k)}}_{j_1,\dots,j_k} = \{x \in V_n \mid x^{(j_1)} = a^{(1)}, \dots, x^{(j_k)} = a^{(k)}\}$ и называемую подфункцией функции *f*. Булева функция $f \in F_n$ называется *k*-аффинной, если существуют наборы $1 \le i_1 < \dots < i_k \le n$, $\mathrm{b} = (b^{(1)}, \dots, b^{(k)}) \in V_k$, такие, что $f^{b^{(1)},\dots,b^{(k)}}_{i_1,\dots,i_k} \in A_{n-k}$.

Определение. *Уровнем аффинности* $\mathrm{la}(f)$ булевой функции $f \in F_n$ называется минимальное число *k*, для которого функция f является *k*-аффинной.

Определение. *Частичным уровнем аффинности* $\mathrm{la}^0(f)$ булевой функции $f \in F_n$ называют минимальное число *k*, для которого существует набор переменных $i_1, \dots, i_k$ такой, что $f^{0,\dots,0}_{i_1,\dots,i_k}$ является аффинной.

Понятие обобщённого уровня аффинности $\mathrm{La}(f)$ булевой функции *f* определяется как минимальная разность между числом переменных функции *f* и размерностью плоскости (смежного класса по подпространству), ограничение на которую совпадает с аффинной функцией.

Обобщенный уровень аффинности, в отличие от уровня аффинности, является аффинным инвариантом, то есть инвариантом относительно действия на функцию полной аффинной группы. Очевидно, что $\mathrm{La}(f) \le \mathrm{la}(f) \le \mathrm{la}^0(f)$ для произвольной булевой функции f.

III. Результаты исследований

A. Алгоритмы определения уровня аффинности

Тривиальный алгоритм определения уровня аффинности булевых функций состоит в проверке аффинности каждой из подфункций булевой функции, которая подаётся ему на вход в виде вектора значений. При этом сначала проверяется, является ли сама функция $f \in F_n$ аффинной, далее проверяются все $2n$ фиксаций одной переменной, далее фиксации двух переменных и так далее. Верхняя оценка сложности этого алгоритма $O(N^2)$, где $N = 2^n$ – длина вектора значений этой функции.

Другой алгоритм с помощью жадного алгоритма находит верхнюю оценку f уровня аффинности, а затем полным перебором ищет плоскость размерности $f - 1$, отображение на которую аффинно. При нахождении первой такой плоскости переходит к размерности $f - 2$ и т.д.

Задача определения уровня аффинности в случае, если количество мономов в АНФ функции ограничено полиномиально от количества переменных, является NP-трудной.

B. Уровень аффинности некоторых классов булевых отображений

Внутри одного класса функции обладают схожими характеристиками. С криптографической точки зрения для противостояния некоторым методам анализа следует использовать функции с достаточно высоким уровнем аффинности. С целью поиска таких функций в работе [2] был исследован уровень аффинности некоторых конструкций и классов булевых отображений.

Конструкция Майорана–Мак-Фарланда и бент-функции

Рассмотрим метод построения булевых функций, образующих так называемый *M*-класс. Пусть $n = s + t$, $\Phi = (\varphi_1, \dots, \varphi_t)$ — некоторое булево отображение $V_s \to V_t$, $h \in F_s$. Конструкция Майорана–Мак-Фарланда определяется как следующая функция $f \in F_n$:

$f(z) = f(x, y) = \langle x, \Phi(y) \rangle \oplus h(y) = \bigoplus_{i=1}^{t} x^{(i)} \varphi_i(y) \oplus h(y)$

,где $z = (x, y)$, $z \in V_n$, $x \in V_t$, $y \in V_s$.

Конструкция Майорана–Мак-Фарланда может рассматриваться как конкатенация 2^s аффинных функций и используется для построения булевых функций с различными свойствами. В частности, в случае n = 2m и взаимооднозначного отображения Φ:

$V_m \to V_m$ функция $f \in M$ является бент-функцией. Для уровня аффинности бент-функций этого класса справедливо соотношение $\mathrm{la}(f) = m$.

Для произвольной бент-функций $f \in B_{2k}$ $\mathrm{la}(f) \geq k$. Аналогичное неравенство выполняется и для платовидной функции порядка 2*k*.

Конструкция Майорана–Мак-Фарланда используется также для построения устойчивых функций. **Определение:** Пусть $f \in F_n$ принадлежит *M*-классу: *t, p* — натуральные числа такие, что $n \geq t > p \geq 0$; отображение Ф: $V_{n-t} \to V_t$ удовлетворяет условию $\mathrm{wt}(\Phi(u)) \geq p$ для любого $u \in V_{n-r}$; *h* — произвольная функция из F_{n-t}. Тогда *f* — *m*-устойчива для некоторого $m \geq p$.

Для подобных устойчивых функций выполнено неравенство $la(f) \leq n - t$.

Конструкция Таранникова

Теорема. Пусть $\frac{2n-7}{3} \leq m \leq n-2$. Тогда существует *m*-устойчивая булева функция *f* из F_n для которой нелинейность достигает максимально возможного значения.

Рекуррентный способ построения искомой функции был предложен Таранниковым Ю. В. в работе [3]. Для этого класса функций доказано неравенство $\mathrm{la}(f) \leq \left[\frac{m+3}{2}\right]$, где *m* – порядок устойчивости функции *f*.

Монотонные булевы функции

Булева функция $f \in F_n$ является монотонной, если для любых двух векторов x, y $\in V_n$ таких, что $x \preccurlyeq y$, выполняется условие $f(x) \leq f(y)$. Класс монотонных булевых функций от *n* переменных обозначим через M_n. Для монотонной булевой функции *f*, $\deg(f) \geq 2$, справедливо равенство:

$$\mathrm{la}(f) = \min\left\{ \min_{\substack{u \in V_n \\ f(u)=1}} wt(u), n - \max_{\substack{v \in V_n \\ f(v)=0}} wt(v) \right\},$$

из чего следует $\mathrm{la}(f) \leq \frac{n}{2}$.

Класс функций с максимально возможным уровнем аффинности

Для любой функции $f \in F_n$ уровень аффинности не может превосходить $n-1$. Это значение достигается тогда и только тогда, когда $f(x_1, \ldots, x_n) = \bigoplus_{i<j} x_i x_j \oplus l_{a,\varepsilon}$, где $l_{a,\varepsilon}$ — произвольная аффинная функция.

Класс симметрических булевых функций

Для симметрической булевой функции $f \in F_n$, то есть функции, значение которой не изменятся при перестановке переменных и, следовательно, зависящей только от веса вектора своих переменных, выполнено $la(f) > n - d$, где $d = \deg(f) > 1$.

C. Уровень аффинности булевой функции и спектральные коэффициенты

Спектральные характеристики булевых функций используются для исследования различных свойств булевых функций и кодов, построенных на их основе. В частности, с помощью коэффициентов Уолша–Адамара можно определить такие параметры булевых функций как нелинейность, корреляционная иммунность и др., в том числе её уровень аффинности.

Пусть $f \in F_n$. Тогда для коэффициентов Уолша–Адамара функции *f* выполняется неравенство $\max_{u \in V_n} |W_f(u)| \geq 2^{n-\mathrm{la}(f)}$.

D. Связь уровня аффинности с криптографическими параметрами булевых функций.

При выборе булевых функций для построении криптографических примитивов принято обращать внимание на следующие параметры, позволяющим противостоять разным видам атак на них:

- уравновешенность;
- высокая алгебраическая степень;
- высокая нелинейность;
- высокий уровень корреляционной иммунности;
- высокий уровень алгебраической иммунности.

Нелинейность N_f булевой функции $f \in F_n$ определяется как расстояние Хэмминга между функцией *f* и множеством A_n.

Для произвольной функции $f \in F_n$ и произвольного $u \in V_n$ преобразование Уолша–Адамара функции *f* определяется выражением

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

При этом набор целых чисел $\{W_f(u) : u \in V_n\}$ называется спектром функции *f*, а каждое число $W_f(u)$ — спектральным коэффициентом Уолша–Адамара функции *f*.

Для случая чётного $n = 2k$ известно, что максимальное значение нелинейности достигается для функций, спектр которых состоит из двух значений коэффициентов Уолша–Адамара: $\pm 2^k$. Такие функции называются максимально-нелинейными или *бент-функциями*.

Кроме бент-функций рассмотрим так называемые *платовидные функции*, спектр которых состоит из трёх возможных значений: $\{f_0, \pm 2^{n-r}\}$, где *n* — количество переменных функции, *r* — некоторое целое число, $0 \leq r \leq n$.

Функция $f \in F_n$ удовлетворяет *строгому лавинному критерию* (SAC), если функция $D_u f = f(x \oplus u) \oplus f(x)$ является уравновешенной для любого $u \in V_n$, такого, что $\mathrm{wt}(u) = 1$. Функция $f \in F_n$ удовлетворяет SAC(*k*), если подфункция $f_{i_1,\ldots,i_k}^{a^{(1)},\ldots,a^{(k)}}$ при любых $1 \leq i_1 < \ldots < i_k \leq n, a \in V_k$ удовлетворяет SAC.

Практически все параметры находятся в жёстких соотношениях между собой, поэтому добиться оптимальных значений каждого из них одновременно невозможно. Существует связь значения уровня аффинности с данными параметрами [2].

Нелинейность. Для любой функции $f \in F_n$ $N_f \leq 2^{n-1} - 2^{n-\mathrm{la}(f)-1}$.

Корреляционная иммунность. Для $f \in F_n$, $\mathrm{wt}(f) \neq 0, 2^n, 2^{n-1}$ $\mathrm{la}(f) > \mathrm{cor}(f)$.

Алгебраическая иммунность. Для любой функции $f \in F_n$ $\mathrm{la}(f) \geq \mathrm{AI}(f) - 1$.

Алгебраическая степень. В общем случае связи между алгебраической степенью функции и уровнем её аффинности не наблюдается.

Лавинные характеристики. Для любой функции $f \in F_n$, удовлетворяющей SAC(t), $\mathrm{la}(f) \geq t$.

E. Асимптотические оценки уровня аффинности для почти всех булевых функций.

Для уровней аффинности булевых функций в работе [4] были найдены следующие асимптотические оценки.

Теорема. Асимптотически при $n \to \infty$ для почти всех функций f из F_n выполнены условия:

$$n - \lfloor \log_2 n \rfloor \leq la(f) \leq n - \lceil \log_2 n \rceil + 1$$
$$n - \lfloor \log_2 n \rfloor \leq La(f) \leq n - \lceil \log_2 n \rceil + 1$$

Таким образом, в случае, когда $n = 2^b$, для почти всех булевых функций имеется два возможных значения уровня (обобщенного уровня) аффинности: $n - b$, $n - b + 1$, иначе единственным возможным значением для уровня (обобщенного уровня) аффинности является число $n - \lfloor \log_2 n \rfloor = n - \lceil \log_2 n \rceil + 1$.

Также была найдена асимптотическая оценка уровней аффинности квадратичных булевых функций (именно на них достигается максимальное значение уровня аффинности). Вероятность того, что для произвольной булевой функции $f \in F_n$, $\deg(f) \leq 2$ $\lfloor M(n) \rfloor \leq \mathrm{la}(f) \leq \lceil M(n) \rceil$, где $M(n) = 2(\log_2 n - \log_2 \log_2 n + \log_2 \frac{e}{2})$, стремится к 1 при $n \to \infty$.

Однако в работах [5], [6] были описаны статистические исследования, которые не смогли подтвердить асимптотические оценки уровня аффинности булевых функций. Так, в [5] был получен обобщенный уровень аффинности для каждого из 150 357 классов аффинной эквивалентности булевых функций от 6 переменных. Как оказалось, он не превосходит значения 3. В работе [6] для исследований были взяты булевы функции от 8 переменных: существенно зависящие от всех своих переменных и уравновешенные. Данные показали, что случайно выбранные булевы функции данного вида в случае $n = 8$ имеют обобщенный уровень аффинности в промежутке [3,4], что позволяет сделать вывод о том, что асимптотическая оценка начинает выполняться только при большем количестве переменных у функции.

Попробуем определить, начиная с какого n булевы функции с обобщенным уровнем аффинности больше $n/2$ преобладают.

Утверждение. В множестве F_n всех булевых функций от n переменных число функций f, удовлетворяющих неравенству $\mathrm{La}(f) > n/2$, составляет более половины множества при $n \geq 12$.

Доказательство. Из [7] известно, что число r-мерных плоскостей пространства V_n равно $2^{n-r}\begin{bmatrix} n \\ r \end{bmatrix}$, где

$$\begin{bmatrix} n \\ r \end{bmatrix} = \begin{cases} \frac{(2^n-1)(2^n-2)\ldots(2^n-2^{r-1})}{(2^r-1)(2^r-2)\ldots(2^r-2^{r-1})}, 1 \leq r \leq n, \\ 1, r = 0. \end{cases}$$

Возьмем любую r-мерную плоскость L пространства V_n. Пусть a_L — количество булевых функций из V_n, ограничение которых на L есть аффинные функции. a_L зависит от числа r и не зависит от выбора L. Тогда количество булевых функций $f \in F_n$, для которых $\mathrm{La}(f) \leq n - r$ будет не больше чем $2^{n-r}\begin{bmatrix} n \\ r \end{bmatrix} a_L$.

Рассмотрим теперь плоскость L вида $\mathrm{F}_2^r \times \{(0,\ldots,0)\}$. Ограничение функции f на эту плоскость является аффинным тогда и только тогда, когда f не содержит мономы длины 2, 3, …, r, состоящие только из переменных $x_1, \ldots, x_r$. Количество функций, обладающих таким свойством, будет равно $2^{2^n - \sum_{i=2}^{r}\binom{r}{i}} = 2^{2^n - 2^r + r + 1} = a_L$. Таким образом получаем, что число функций, имеющих аффинное ограничение на r-мерных плоскостях, не больше чем $2^{n-r}\begin{bmatrix} n \\ r \end{bmatrix} 2^{2^n - 2^r + r + 1}$, а их доля относительно всех функций из F_n равна $2^{n-r}\begin{bmatrix} n \\ r \end{bmatrix} 2^{-2^r + r + 1}$.

Далее, поскольку каждый множитель в числителе дроби, определяющей $\begin{bmatrix} n \\ r \end{bmatrix}$, меньше 2^n, а каждый множитель в знаменателе больше или равен 2^{r-1}, то $\begin{bmatrix} n \\ r \end{bmatrix} < 2^{n(r-1)-(r-1)^2} = 2^{n(r-1)-r^2+2r-1}$. Отсюда доля функций, имеющих аффинное ограничение на r-мерных плоскостях, меньше чем $2^{n(r-1)-r^2+2r-1+n-r-2^r+r+1} = 2^{-2^r + r(n+2-r)}$.

Положим $r = n/2$. Тогда неравенство $2^{\frac{n^2}{4} + n - 2^{n/2}} < \frac{1}{2}$ выполнено при $n \geq 12$.

IV. Заключение

В статье представлен обзор полученных на данный момент результатов исследований двух важных параметров булевых функций. Были рассмотрены свойства уровня аффинности, его связь с другими параметрами и с криптографическими свойствами булевых функций.

Для криптографии представляют ценность функции с достаточно высоким уровнем аффинности. При изучении некоторых конструкций и классов булевых функций оказалось, что этим свойством обладают симметрические, платовидные и бент-функции, а также был найден класс функций с максимально возможным уровнем аффинности. Известно, что асимптотически при стремлении количества переменных n функции f к бесконечности ее уровень аффинности принимает высокие значения, и доля функций с $\mathrm{La}(f) > n/2$ составляет более половины числа всех функций из F_n уже при $n = 12$, однако конкретных функций с высоким обобщенным уровнем аффинности до сих пор найдено не было. Одной из актуальных задач в этой области является построение наиболее эффективных алгоритмов поиска таких функций.

Библиография

[1] O. A. Logachev, V. V. Yashchenko, and M. P. Denisenko, “Local Affinity of Boolean Mappings”, Boolean Functions in Cryptology and Information Security, IOS Press, 2008, pp. 148-172.

[2] М. Л. Буряков, “Алгебраические, комбинаторные и криптографические свойства параметров аффинных ограничений булевых функций”, Диссертация на соискание ученой степени кандидата физико-математических наук, Москва, 2008.

[3] Ю. В. Тарannиков, “О корреляционно-иммунных и устойчивых булевых функциях”, Математические вопросы кибернетики, Физматлит, 2002, вып. 11, с. 91–148.

[4] О. А. Логачев, “О значениях уровня аффинности для почти всех булевых функций”, ПДМ, 2010, № 3, с. 17–21.

[5] А. И. Огнев, “Определение значения обобщенного уровня аффинности классов аффинной эквивалентности булевых функций от 6 переменных”, 2010, неопубликованная.

[6] А. И. Огнев, “Некоторые оценки параметров локальных аффинностей булевых функций”, Сборник тезисов лучших дипломных работ 2012 года, издательский отдел факультета ВМК МГУ, 2012, с. 190.

[7] Ф. Дж. Мак-Вильямс и Н. Дж. А. Слоэн, “Теория кодов, исправляющих ошибки”, Связь, 1979.

Some properties of affine restrictions of Boolean functions and mappings

Mishanova E. M.

***Abstract*—The article summarizes a number of studies of affine restrictions of Boolean functions and mappings. I study properties of the level and generalized level of affinity, as well as their relation to the parameters that describe the other properties of Boolean functions. Asymptotic estimates are given and I consider targets for further work in this area.**

***Key words*—Boolean mappings, cryptography, generalized level of affinity, level of affinity, system of Boolean equations.**