Пример 1. К.б.п.ф. $f \sim (\mathbf{1}_1|\mathbf{1}_3, 2)$ зависит несущественно от первой переменной. Её таблица истинности и многочлен Жегалкина такие же, как для пороговой функции $((1,1,1),1)$, т. е. $x_2x_3 + x_2x_4 + x_3x_4$.

Пример 2. К.б.п.ф. $g_1 \sim (\mathbf{1}_2|\mathbf{1}_3, 8)$ имеет многочлен Жегалкина $x_3x_4x_5$, хотя при порогах 7 или 9 с той же матрицей квадратичной формы соответствующие функции g_2 и g_3 зависят существенно от всех пяти переменных и имеют многочлены Жегалкина $x_1x_2x_3x_4 + x_1x_2x_3x_5 + x_1x_2x_4x_5 + x_3x_4x_5 + x_1x_2x_3x_4x_5$ и $x_1x_3x_4x_5 + x_2x_3x_4x_5 + x_1x_2x_3x_4x_5$ соответственно. При этом функция g_1 является линейной пороговой со структурой $((0,0,1,1,1),2)$, а функции g_2 и g_3 — линейными пороговыми со структурами $((1,1,3,3,3),7)$ и $((1,1,3,3,3),9)$ соответственно. Кроме того, обе функции допускают декомпозиции $g_2 = x_1x_2(x_3x_4 + x_3x_5 + x_4x_5 + x_3x_4x_5)$ и $g_3 = (x_1 + x_2 + x_1x_2)x_3x_4x_5$.

Приведённые примеры показывают, что даже в случае очень простых квадратичных форм задаваемые ими к.б.п.ф. могут сильно отличаться в смысле существенной зависимости от переменных при небольших (последовательных) изменениях порога. Кроме того, интерес представляет нахождение пороговой степени (см. определение в [1]) к.б.п.ф. В заключение отметим, что даже для линейной пороговой булевой функции задача определения существенной зависимости переменной является NP-полной [6, теорема 9.26, с. 436], что повышает значимость разработки эвристических методов её решения.

ЛИТЕРАТУРА

1. *Подольский В. В.* Оценки весов персептронов (полиномиальных пороговых булевых функций): автореф. дис. ... канд. физ.-мат. наук. М.: МГУ им. М. В. Ломоносова, 2009.
2. *Шурупов А. Н.* О функциональной разделимости булевых пороговых функций // Дискретная математика. 1997. Т. 9. Вып. 2. С. 59–73.
3. *Хачиян Л. Г.* Полиномиальный алгоритм в линейном программировании // Докл. АН СССР. 1979. Т. 244. № 5. С. 1033–1096.
4. *Dreo J., Petrowski A., Siarry P., and Taillard E.* Metaheuristics for Hard Optimisation. Methods and Case Studies. Springer, 2006. 372 p.
5. *Хохлюк В. И.* Прямой метод целочисленной оптимизации. Новосибирск: Ин-т математики им. С. Л. Соболева, 2002. 38 с.
6. *Crama Y. and Hammer P.* Boolean Functions. Theory, Algorithms and Applications. Cambridge University Press, 2011.

УДК 519.7 DOI 10.17223/2226308X/8/19

О СВОЙСТВАХ МНОЖЕСТВА ЗНАЧЕНИЙ ПРОИЗВОЛЬНОЙ ВЕКТОРНОЙ БУЛЕВОЙ ФУНКЦИИ[1]

Г. И. Шушуев

Исследуются свойства множества значений производных векторной булевой функции из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$. Получены достаточные условия того, что множество всех значений производных некоторой булевой функции совпадает с $\mathbb{F}_2^n$. Этот результат связан с некоторым открытым вопросом о метрических свойствах APN-функций.

[1]Работа поддержана грантом РФФИ, проект № 15-31-20635.

Ключевые слова: *векторная булева функция, дифференциально δ-равномерная функция, APN-функция.*

В работе рассматриваются векторные булевы функции $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, которые также известны как S-блоки. Они играют центральную роль для криптографической стойкости блочных шифров.

В 1994 г. K. Nyberg [1] ввела понятие дифференциально δ-равномерных векторных булевых функций. Векторная булева функция $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ называется *дифференциально δ-равномерной*, если для любого ненулевого вектора $a \in \mathbb{F}_2^n$ и любого вектора $b \in \mathbb{F}_2^n$ уравнение $F(x) \oplus F(x \oplus a) = b$ имеет не более δ решений, где δ — целое положительное число. *Порядком* дифференциальной равномерности функции F назовём минимальное возможное δ, такое, что F — дифференциально δ-равномерная функция.

Чем меньше порядок дифференциальной равномерности S-блока, который используется в шифре, тем выше стойкость шифра к дифференциальному криптоанализу [2]. Минимальное возможное значение, которое может принимать δ, — это 2. Если $\delta = 2$, то дифференциально δ-равномерная функция называется APN-функцией (*Almost Perfect Nonlinear*). Для векторной булевой функции F и любого ненулевого вектора $a \in \mathbb{F}_2^n$ определим множество

$$B_a(F) = \{F(x) \oplus F(x \oplus a) : x \in \mathbb{F}_2^n\}.$$

Максимальная достижимая мощность множества $B_a(F)$ равна 2^{n-1}. В частности, если при любом ненулевом векторе a выполнено $|B_a(F)| = 2^{n-1}$, то функция F является APN [3].

В работе [4] исследовалось расстояние между различными APN-функциями, в связи с этим была выдвинута следующая гипотеза.

Гипотеза 1. Если F — APN-функция от n переменных, то выполнено

$$\forall x' \in \mathbb{F}_2^n \left(\bigcup_{a \in \mathbb{F}_2^n, a \neq 0} (B_a(F) \oplus F(x' \oplus a)) = \mathbb{F}_2^n \right).$$

Для доказательства этой гипотезы требуется рассматривать объединение множеств $B_a(F)$. В данной работе исследуются некоторые свойства множества значений произвольной векторной булевой функции из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$, а именно множество значений её производных. Полученные результаты помогут в изучении метрических свойств класса APN-функций.

Суммой двух множеств $A, B \subseteq \mathbb{F}_2^n$ назовём множество всех попарных сумм элементов этих множеств: $A \oplus B = \{a \oplus b : a \in A, b \in B\}$. Сумма вектора $x \in \mathbb{F}_2^n$ и множества $A \subseteq \mathbb{F}_2^n$ — сдвиг множества A: $x \oplus A = \{x \oplus a : a \in A\}$. Множество всех значений векторной булевой функции $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ называется *образом* функции F и обозначается $\mathrm{im}(F)$.

Лемма 1. Пусть $A, B \subseteq \mathbb{F}_2^n$, $|A| \geqslant 2^{n-1}$ и $|B| \geqslant 2^{n-1} + 1$. Тогда $A \oplus B = \mathbb{F}_2^n$.

Теорема 1. Пусть $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ — векторная булева функция. Тогда:

1) если $2^{n-1} < |\mathrm{im}(F)| < 2^n$, то

$$\bigcup_{a \in \mathbb{F}_2^n, a \neq 0} B_a(F) = \mathbb{F}_2^n;$$

2) если $|\mathrm{im}(F)| = 2^n$, т. е. F является перестановкой, то

$$\bigcup_{a\in\mathbb{F}_2^n, a\neq 0} B_a(F) = \mathbb{F}_2^n \backslash \{0\}.$$

Условие на мощность образа функции не может быть ослаблено. Существуют функции F, у которых мощность образа равна $|\mathrm{im}(F)| = 2^{n-1}$ и выполнено $\bigcup\limits_{a\in\mathbb{F}_2^n, a\neq 0} B_a(F) \neq \mathbb{F}_2^n$. Например, такова APN-функция $F : \mathbb{F}_2^3 \to \mathbb{F}_2^3$, заданная вектором значений $(0, 0, 1, 2, 1, 4, 2, 4)$. Для неё $|\mathrm{im}(F)| = 2^2$, а $\bigcup\limits_{a\in\mathbb{F}_2^n, a\neq 0} B_a(F) = \mathbb{F}_2^n \backslash \{7\}$.

Теорема показывает, как ведёт себя объединение множеств $B_a(F)$, при каких условиях на образ функции F объединение даёт всё пространство $\mathbb{F}_2^n$, а при каких нет.

ЛИТЕРАТУРА

1. *Nyberg K.* Differentially uniform mappings for cryptography // LNCS. 1994. V. 765. P. 55–64.
2. *Biham E. and Shamir A.* Differential cryptoanalysis of DES-like cryptosystems // J. Cryptology. 1991. No. 4. P. 3–72.
3. *Beth T. and Ding C.* On almost perfect nonlinear permutations // LNCS. 1994. V. 765. P. 65–76.
4. *Шушуев Г. И.* Векторные булевы функции на расстоянии один от APN-функций // Прикладная дискретная математика. Приложение. 2014. № 7. С. 36–37.