2. *Mittenthal L.* Block substitutions using orthomorphic mappings // Adv. Appl. Math. 1995. V. 16. Iss. 1. P. 59–71.
3. *Beaulieu R., Shors D., Smith J., et al.* The Simon and Speck Families Of Lightweight Block Ciphers. Cryptology ePrint Archive, Report 2013/404, 2013.

УДК 519.7 DOI 10.17223/2226308X/13/8

# О РАЗЛОЖЕНИИ ВЕКТОРНОЙ БУЛЕВОЙ ФУНКЦИИ В КОМПОЗИЦИЮ ДВУХ ВЕКТОРНЫХ ФУНКЦИЙ[1]

Г. М. Пинтус

Исследуется возможность представления векторной булевой функции в виде композиции двух векторных булевых функций меньшей алгебраической степени. Вводится понятие разложимости векторной булевой функции. Изучен вопрос сохранения разложимости при расширенном аффинном преобразовании. Представлена конструкция векторной булевой функции третьей степени от произвольного числа переменных, являющейся разложимой. Проведён вычислительный эксперимент, в результате которого показано, что все кубические векторные булевы функции от трёх переменных являются разложимыми.

**Ключевые слова:** *векторная булева функция, декомпозиция, пороговая реализация.*

Атаки по сторонним каналам [1] — вид атак, целью которых является нахождение уязвимостей в реализации криптографической системы. На данный момент эти атаки являются одними из наиболее эффективных среди всех видов криптоанализа. В атаках по сторонним каналам используется информация, полученная при отслеживании перепадов напряжений, времени выполнения процессов, электромагнитного излучения или звуков при проводимых алгоритмом вычислениях.

Пороговая реализация [2] является контрмерой по отношению к атакам по сторонним каналам, она разделяет наборы входных данных и используемые векторные булевы функции на части, позволяя скрыть различия между операциями. Таким образом, если разбиение удовлетворяет ряду условий, при работе алгоритма не происходит утечки информации, которая может быть использована в атаке по сторонним каналам.

В данном методе необходимо построить разбиение для векторной булевой функции определённым образом, что не всегда удаётся сделать. Однако придуман способ решения проблемы, использующий построение разбиения для более простых функций, композицией которых является исходная векторная булева функция.

В настоящей работе анализируется возможность представления векторных булевых функций в виде композиции векторных булевых функций меньших степеней. Рассмотрены векторные булевы функции от трёх переменных с алгебраической степенью равной трём и возможность их представления в виде композии двух векторных булевых функций алгебраической степени два.

Так как важно сохранение свойств при преобразованиях, а одним из наиболее распространённых является расширенное аффинное преобразование, мы исследуем вопрос сохранения разложимости векторной булевой функции при расширенной аффинной эквивалентности.

*Векторной булевой функцией* ($(n, m)$-функцией) $F$ называется произвольное отображение $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. В случае $m = 1$ говорят, что $F$ — *булева функция от* $n$ *пере-*

[1]Работа выполнена при поддержке Лаборатории криптографии JetBrains Research.

*менных*; $(n,m)$-функция $F$ может быть задана набором из $m$ координатных булевых функций от $n$ переменных: $F(x) = (f_1(x), f_2(x), \ldots, f_m(x))$, $x \in \mathbb{F}_2^n$. Любую $(n,m)$-функцию можно единственным образом записать в виде *полинома Жегалкина*, или *алгебраической нормальной формы* (АНФ):

$$F(x_1, \ldots, x_n) = \Big( \bigoplus_{k=1}^{n} \bigoplus_{i_1,\ldots,i_k} a_{i_1,\ldots,i_k} x_{i_1} \cdot \ldots \cdot x_{i_k} \Big) \oplus a_0,$$

где для каждого $k$ индексы $i_1, \ldots, i_k$ попарно различны и множества $\{i_1, \ldots, i_k\}$ являются всеми различными непустыми подмножествами множества $\{1, \ldots, n\}$; коэффициенты $a_{i_1,\ldots,i_k}, a_0$ принимают значения из $\mathbb{F}_2^m$. *Алгебраической степенью* $\deg(F)$ функции $F$ называется количество переменных в самом длинном слагаемом АНФ, коэффициент при котором не равен нулевому вектору. Функция степени не выше 1 называется *аффинной*, при этом в случае $a_0 = 0$ функция *линейна*.

Две $(n,n)$-функции $F$ и $G$ называются *расширенно аффинно эквивалентными* (EA-эквивалентными), если существуют две аффинные $(n,n)$-подстановки $A, B$ на множестве $\mathbb{F}_2^n$ и аффинная $(n,n)$-функция $C$, такие, что $G(x) = (B \circ F \circ A)(x) + C(x)$, $x \in \mathbb{F}_2^n$.

Пусть $F$ — такая $(n,n)$-функция, что существуют $(n,n)$-функции $G, H$, для которых $\max\{\deg(G), \deg(H)\} < \deg(F)$ и $F(x) = G(H(x))$ для всех $x \in \mathbb{F}_2^n$. Функцию $F$ степени $d > 2$, допускающую такую декомпозицию, будем называть *разложимой*.

**Теорема 1.** Пусть $(n,n)$-функция $F$ степени $d > 2$ разложима. Тогда $(n,n)$-функция $F' = A_2 \circ F \circ A_1$, где $A_1, A_2$ — произвольные аффинные $(n,n)$-подстановки, также разложима. Если $F$ представима в виде композиции двух $(n,n)$-функций $G, H$ степени меньше $d$, таких, что функция $H$ обратима и $\deg(H^{-1}) \leqslant \max\{\deg(G), \deg(H)\}$, то $(n,n)$-функция $F'' = F + A_0$ разложима для любой аффинной $(n,n)$-функции $A_0$.

Получена конструкция, которая позволяет для любого $n$ построить класс разложимых векторных булевых функций третьей степени.

**Теорема 2.** Пусть $i, j, p, q \in \{1, \ldots, n\}$, $i \neq j$, $p \neq q$; $\{l_k : k = 1, \ldots, n\}$ и $\{l'_r : r = 1, \ldots, n\}$ — наборы произвольных линейных булевых функций от $n$ переменных, такие, что $\deg(x_p x_q (l_i(x) + l_j(x))) = 3$; $Y(x) = (y_1(x), \ldots, y_n(x))$, где $y_k(x) = x_p x_q + l_k(x)$ при $k = 1, \ldots, n$, $x \in \mathbb{F}_2^n$. Тогда разложимой является векторная булева функция $F(x)$, определённая следующим образом:

$$F(x) = \begin{pmatrix} f_1(x) \\ f_2(x) \\ \ldots \\ f_n(x) \end{pmatrix} = \begin{pmatrix} x_p x_q (l_i(x) + l_j(x)) + x_p x_q + l_i(x) l_j(x) + l'_1(Y(x)) \\ x_p x_q (l_i(x) + l_j(x)) + x_p x_q + l_i(x) l_j(x) + l'_2(Y(x)) \\ \ldots \\ x_p x_q (l_i(x) + l_j(x)) + x_p x_q + l_i(x) l_j(x) + l'_n(Y(x)) \end{pmatrix}.$$

## ЛИТЕРАТУРА

1. *Bhunia S. and Tehranipoor M.* Hardware Security. A Hands-On Learning Approach. Elsevier Inc., 2019. 526 p.
2. *Nikova S., Rechberger C., and Rijmen V.* Threshold implementations against side-channel attacks and glitches // Inform. Commun. Technol. 2006. No. 4307. P. 529—546.