УДК 519.7 DOI 10.17223/2226308X/15/9

О КОРРЕЛЯЦИОННО-ИММУННЫХ ФУНКЦИЯХ С МАКСИМАЛЬНОЙ АЛГЕБРАИЧЕСКОЙ ИММУННОСТЬЮ[1]

И. С. Хильчук, Д. А. Зюбина, Н. Н. Токарева

Рассматривается геометрическое представление корреляционно-иммунных булевых функций с максимальной алгебраической иммунностью. Найдено пересечение классов функций с максимальной алгебраической иммунностью и функций, обладающих корреляционной иммунностью, от малого числа переменных. Для $n = 3, 4, 5$ произведена классификация таких функций.

Ключевые слова: *булевы функции, алгебраическая иммунность, корреляционная иммуность, булев куб.*

Булевы функции являются основными компонентами симметричных шифров, их криптографические свойства обеспечивают стойкость шифра к различным видам криптоанализа. Например, в работе [1] рассмотрены связи корреляционной иммунности с другими свойствами булевых функций. В данной работе основным рассматриваемым свойством является алгебраическая иммунность, обеспечивающая стойкость шифра к алгебраическому криптоанализу, введённому Н. Куртуа в 2003 г. [2]. Корреляционная иммунность используется в качестве вспомогательного свойства для сокращения числа рассматриваемых функций и поиска закономерностей и интересных структур, так как накладывает ограничения на расположение носителя булевой функции в булевом кубе.

Так как полный перебор множества всех булевых функций затруднён, наибольший интерес представляют подходы, при которых булевы функции с нужными свойствами находятся с помощью средств машинного обучения, таких, как генетические алгоритмы [3], или строятся, как, например, в [4]. В данной работе изучается способ построения булевых функций от большего числа переменных на основе функций от меньшего числа переменных с сохранением криптографических свойств исходных функций. Используется геометрическое представление булевой функции: носитель булевой функции рассматривается как подможество вершин булева куба соответствующей размерности.

Любую булеву функцию можно единственным образом записать в *алгебраической нормальной форме* (АНФ, полином Жегалкина):

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

где при каждом k все индексы $i_1, \ldots, i_k$ различны и параметры $a_0, a_{i_1,\ldots,i_k}$ принимают значения 0 или 1.

Носитель булевой функции — множество всех векторов, на которых функция принимает значение 1:

$$\mathrm{supp}(f) = \{x \in \mathbb{Z}_2^n : f(x) = 1\}.$$

Булев куб — граф $\mathbb{E}^n$, вершинами которого являются все двоичные векторы длины n, т. е. $V = \{(x_1, \ldots, x_n) : x_i \in \mathbb{Z}_2\}$, а рёбрами соединяются только те векторы, расстояние Хэмминга между которыми равно единице. Число n называется *размерностью* булева куба.

[1]Работа выполнена в рамках госзадания ИМ СО РАН (проект № FWNF-2022-0018).

Весом Хэмминга $\mathrm{wt}(f)$ булевой функции f от n переменных называется число ненулевых координат её вектора значений. *Гранью размерности* k в булевом кубе $\mathbb{E}^n$ называется множество

$$\Gamma^{a_1,\ldots,a_{n-k}}_{i_1,\ldots,i_{n-k}} = \{x_{i_1} = a_1, \ldots, x_{i_{n-k}} = a_{n-k}\}.$$

Булева функция $f(x)$ от n переменных называется *сбалансированной*, если принимает каждое из значений 0 и 1 ровно 2^{n-1} раз [5].

Алгебраической иммунностью $\mathrm{AI}(f)$ булевой функции f от n переменных называется минимальное число d, такое, что существует не тождественно равная нулю булева функция g от n переменных степени d, для которой выполняется $f \cdot g = 0$ или $(f+1)g = 0$ [5]. Высокая алгебраическая иммунность обеспечивает стойкость шифра к алгебраическому криптоанализу. Известна оценка сверху алгебраической иммунности булевой функции от n переменных: $\mathrm{AI}(f) \leqslant \lceil n/2 \rceil$ [2].

Булева функция f от n переменных называется *корреляционно-иммунной порядка* r, $1 \leqslant r \leqslant n$, если для любой её подфункции $f^{a_1,\ldots,a_r}_{i_1,\ldots,i_r}$, полученной фиксацией r переменных, выполняется равенство

$$\mathrm{wt}(f^{a_1,\ldots,a_r}_{i_1,\ldots,i_r}) = \frac{\mathrm{wt}(f)}{2^r}.$$

Эквивалентное определение: булева функция f от n переменных является корреляционно-иммунной порядка $n-k$, $1 \leqslant k \leqslant n$, если любой грани $\Gamma^{a_1,\ldots,a_{n-k}}_{i_1,\ldots,i_{n-k}}$ булева куба $\mathbb{E}^n$ размерности k принадлежит одинаковое число точек носителя функции f, а именно $2^{-(n-k)}\mathrm{wt}(f)$ точек.

Так как корреляционно-иммунная порядка m булева функция является также корреляционно-иммунной порядка ℓ для всех $\ell < m$ [6], можем ввести обозначение для максимального порядка корреляционной иммунности:

$$\mathrm{CI}(f) = \max\{m \in \mathbb{N} : f \text{ — корреляционно-иммунная порядка } m\}.$$

Пусть f — булева функция от n переменных. *Геометрическим представлением* булевой функции f назовём подграф булева куба $\mathbb{E}^n$, индуцированный носителем функции f. Напомним, что два графа F и G называются *изоморфными*, если существует биекция ψ на множествах их вершин, такая, что образы $\psi(u)$ и $\psi(v)$ в графе G смежны тогда и только тогда, когда смежны вершины u и v в графе F.

Два подграфа G_1 и G_2 булева куба $\mathbb{E}^n$, индуцированные носителями функций f_1 и f_2 соответственно, назовём *изоморфными по метрическому вложению*, если найдётся автоморфизм $\varphi : \mathbb{E}^n \to \mathbb{E}^n$ булева куба $\mathbb{E}^n$, под действием которого G_1 переходит в G_2. Напомним, что любой автоморфизм булева куба $\mathbb{E}^n$ как графа является изометрией $\mathbb{E}^n$ относительно расстояния Хэмминга.

1. Булевы функции от трёх переменных

Для $n = 3$ получена полная классификация булевых функций с корреляционной иммунностью порядков 3, 2, 1. Всего существуют:

- 2 функции порядка 3 — функции-константы;
- 4 функции порядка 2 — функции-константы и функции-счётчики чётности;
- 18 функций порядка 1.

Из всех этих функций ни одна не имеет максимально возможного значения алгебраической иммунности (т. е. $\mathrm{AI}(f) < 2$).

2. Булевы функции от четырёх переменных

Исследуем пересечение множеств булевых функций от четырёх переменных с максимальной алгебраической иммунностью (равной 2) и с максимальным порядком корреляционной иммунности 1. Заметим, что среди функций от четырёх переменных с максимальной алгебраической иммунностью не существует функций с более высоким максимальным порядком корреляционной иммунности.

В этом пересечении лежат 392 функции, среди которых функции веса 6 (96 функций), 8 (200 функций) и 10 (96 функций), при этом функции веса 6 совпадают с инверсиями функций веса 10. Ограничения на вес функций накладывают рассматриваемые характеристики: корреляционная иммунность требует чётного веса, а для того, чтобы алгебраическая иммунность имела максимальный показатель $\mathrm{AI}(f) = 2$, необходимо, чтобы выполнялись следующие ограничения: $\mathrm{wt}(f) \geqslant \sum\limits_{i=0}^{d} \binom{n}{i}$ и $\mathrm{wt}(f \oplus 1) \geqslant \sum\limits_{i=0}^{d} \binom{n}{i}$, где $d = \mathrm{AI}(f) - 1 = 1$, $n = 4$.

Будем рассматривать только функции, которые принимают значение 1 на нулевом векторе: 36 функций веса 6, 100 функций веса 8, 60 функций веса 10. Мы можем это сделать, так как инвертирование функции не изменяет показатели её алгебраической и корреляционной иммунности.

Заметим, что все функции разбиваются на классы сообразно своему геометрическому представлению (или виду АНФ). Переход от одной булевой функции к другой внутри класса осуществляется переобозначением переменных.

Произведена классификация данных булевых функций и написана программа, с помощью которой на основе рассматриваемых 196 функций от четырёх переменных построены функции от шести переменных и проверена их алгебраическая и корреляционная иммунность.

2.1. Булевы функции веса 6 с $\mathrm{AI}(f) = 2$, $\mathrm{CI}(f) = 1$

Рассмотрим функции веса 6 с $\mathrm{AI}(f) = 2$, $\mathrm{CI}(f) = 1$, принимающие значение 1 на нулевом векторе, и индуцированные их носителями подграфы булева куба $\mathbb{E}^4$ (рис. 1). Здесь и далее метками у тонких линий обозначены расстояния между несмежными вершинами графа. Подграфы данного вида симметричны относительно вертикальной оси, мы не различаем симметричные вершины.

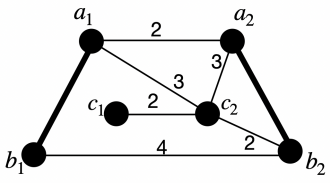


Рис. 1. Подграф из G_6

Все подграфы, индуцированные носителями таких функций, изоморфны по вложению между собой. Обозначим данное множество индуцированных подграфов как G_6.

Утверждение 1. Булева функция f от четырёх переменных веса 6, принимающая значение 1 на нулевом векторе, имеет характеристики $\mathrm{AI}(f) = 2$ и $\mathrm{CI}(f) = 1$, если и только если индуцированный её носителем подграф булева куба $\mathbb{E}^4$ изоморфен по вложению графу на рис. 1. От того, какой вершиной индуцированного носителем подграфа является нулевой вектор булева куба, зависит вид алгебраической нормальной формы функции f:

1) нулевой вектор — изолированная вершина (12 функций), пример АНФ:

$$x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus x_4 \oplus x_3 \oplus x_2 \oplus x_1 \oplus 1;$$

2) нулевой вектор — вершина a_i, $i = 1, 2$ (12 функций), пример АНФ:

$$x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_3x_4 \oplus x_2x_4 \oplus x_4 \oplus x_3 \oplus x_2 \oplus 1;$$

3) нулевой вектор — вершина b_i, $i = 1, 2$ (12 функций), пример АНФ:

$$x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_3x_4 \oplus x_4 \oplus x_3 \oplus x_2 \oplus 1.$$

2.2. Булевы функции веса 10 с $\mathrm{AI}(f) = 2$, $\mathrm{CI}(f) = 1$

Подграфы булева куба, индуцированные носителями функций веса 10 с $\mathrm{AI}(f) = 2$ и $\mathrm{CI}(f) = 1$, принимающих значение 1 на нулевом векторе, также изоморфны по вложению между собой; обозначим множество таких подграфов как G_{10} (рис. 2).

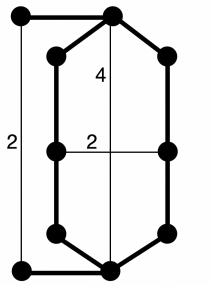


Рис. 2. Подграф из G_{10}

Утверждение 2. Булева функция f от четырёх переменных веса 10, принимающая значение 1 на нулевом векторе, имеет характеристики $\mathrm{AI}(f) = 2$ и $\mathrm{CI}(f) = 1$, если и только если индуцированный её носителем подграф булева куба $\mathbb{E}^4$ изоморфен по вложению графу на рис. 2. От того, какой вершиной индуцированного носителем подграфа является нулевой вектор булева куба, зависит вид алгебраической нормальной формы функции f:

1) нулевой вектор — вершина степени 1 (12 функций), пример АНФ:

$$x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2 \oplus x_3 \oplus x_4 \oplus 1;$$

2) нулевой вектор — вершина степени 2, равноудалённая от вершин степени 3 (12 функций), пример АНФ:

$$x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_2 \oplus x_1x_4 \oplus x_2x_3 \oplus x_3 \oplus x_4 \oplus 1;$$

3) нулевой вектор — вершина степени 2, не равноудалённая от вершин степени 3 (24 функции), пример АНФ:

$$x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus$$

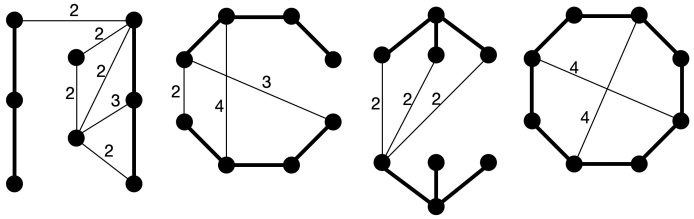
$$\oplus x_1 \oplus x_4 \oplus 1;$$

4) нулевой вектор — вершина степени 3 (12 функций), пример АНФ:

$$x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_4 \oplus 1.$$

2.3. Булевы функции веса 8 с $\mathrm{AI}(f) = 2$, $\mathrm{CI}(f) = 1$

Индуцированные носителями функций веса 8 с $\mathrm{AI}(f) = 2$, $\mathrm{CI}(f) = 1$ подграфы имеют четыре возможных вида, обозначим их G_8^i, $i = 1, 2, 3, 4$ (рис. 3). Подграфы в каждом из G_8^i, $i = 1, 2, 3, 4$, изоморфны по вложению между собой.



а *б* *в* *г*

Рис. 3. Подграфы из G_8

Утверждение 3. Булева функция f от четырёх переменных веса 8, принимающая значение 1 на нулевом векторе, имеет характеристики $\mathrm{AI}(f) = 2$ и $\mathrm{CI}(f) = 1$, если и только если индуцированный её носителем подграф булева куба $\mathbb{E}^4$ изоморфен по вложению одному из графов на рис. 3. От того, какой вид имеет индуцированный носителем функции подграф и какой вершиной этого подграфа является нулевой вектор булева куба, зависит вид алгебраической нормальной формы функции f:

1. Два 2-пути и две изолированные вершины (рис. 3, *а*):
   а) нулевой вектор — вершина степени 2 (6 функций), пример АНФ:
   $$x_1x_2 \oplus x_3 \oplus x_4 \oplus 1;$$
   б) нулевой вектор — вершина степени 1 (12 функций), пример АНФ:
   $$x_1x_2 \oplus x_2 \oplus x_3 \oplus x_4 \oplus 1;$$
   в) нулевой вектор — изолированная вершина (6 функций), пример АНФ:
   $$x_3x_4 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus 1.$$
2. Два 3-пути (рис. 3, *б*):
   а) нулевой вектор — вершина степени 2 (24 функции), пример АНФ:
   $$x_1x_2 \oplus x_2x_3 \oplus x_3 \oplus x_4 \oplus 1;$$
   б) нулевой вектор — вершина степени 1н (24 функции), пример АНФ:
   $$x_1x_2 \oplus x_3x_4 \oplus x_2 \oplus x_3 \oplus x_4 \oplus 1.$$
3. Две вершины степени 3 (рис. 3, *в*):
   а) нулевой вектор — вершина степени 3 (4 функции), пример АНФ:
   $$x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_4 \oplus 1;$$
   б) нулевой вектор — вершина степени 1 (12 функций), пример АНФ:
   $$x_2x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus x_1 \oplus x_2 \oplus x_3 \oplus 1.$$
4. Цикл длины 8 (рис. 3, *г*), пример АНФ:
   $$x_1x_2 \oplus x_1x_4 \oplus x_2x_3 \oplus x_3x_4 \oplus x_3 \oplus x_4 \oplus 1.$$

3. Булевы функции от пяти переменных

При $n = 5$ получен полный список булевых функций с максимальной алгебраической иммунностью ($\mathrm{AI}(f) = 3$) — всего их 197 765 122. Из них 96 768 функций имеют корреляционную иммунность порядка 1. Функций с более высоким порядком корреляционной иммунности и с максимальной алгебраической иммунностью не существует.

4. Булевы функции от шести переменных

Для перехода к функциям от шести переменных мы заменяем каждый вектор булева куба $\mathbb{E}^4$ на грань размерности 2. В таком случае, если вектор булева куба $\mathbb{E}^4$ принадлежал носителю исходной функции от четырёх переменных, существуют пять вариантов расположения точек носителя в новой грани размерности 2:

— все векторы новой грани принадлежат носителю функции от шести переменных;
— три вектора новой грани принадлежат носителю;
— два вектора новой грани на расстоянии 1 друг от друга принадлежат носителю;
— два вектора новой грани на расстоянии 2 друг от друга принадлежат носителю;
— один вектор новой грани принадлежит носителю функции от шести переменных.

Исследован способ построения, при котором все вершины, принадлежащие носителю, заменяются на грань одного и того же вида. При этом необходимо учитывать, что для сохранения максимального порядка корреляционной иммунности 1 необходимо, чтобы каждой грани булева куба $\mathbb{E}^6$ размерности 5 принадлежало одинаковое число точек носителя. С помощью программы мы проверили алгебраическую иммунность всех полученных функций от шести переменных и выяснили, что все варианты (с учётом ограничений, накладываемых корреляционной иммунностью) позволяют построить функцию от шести переменных с сохранением показателей алгебраической и корреляционной иммунности исходной булевой функции от четырёх переменных. Однако ни в одном случае не наблюдался рост алгебраической иммунности до максимально возможного показателя $\mathrm{AI}(f) = 3$ для функций от шести переменных.

Заключение

В работе получена полная классификация булевых функций от трёх, четырёх и пяти переменных с максимальной алгебраической иммунностью и обладающих корреляционной иммунностью. Исследован способ построения булевых функций большей размерности на основе функций меньшей размерности с заданными свойствами с сохранением этих свойств. В дальнейшем планируется рассмотреть другие возможности построения функций от шести переменных на основе геометрического представления функций от четырёх переменных, добиться повышения показателя алгебраической иммунности.

ЛИТЕРАТУРА

1. *Тарасников Ю. В.* О корреляционно-иммунных и устойчивых булевых функциях // Математические вопросы кибернетики. Вып. 11. М.: Физматлит, 2002. С. 91–148.
2. *Courtois N. and Meier W.* Algebraic attack on stream ciphers with linear feedback // LNCS. 2003. V. 2656. P. 345–359.
3. *Mariot L., and Leporati A.* A genetic algorithm for evolving plateaued cryptographic Boolean functions // LNCS. 2015. V. 9477. P. 33–45.
4. *Sun L. and Fu F.-W.* Constructions of balanced odd-variable rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity // Theor. Comput. Sci. 2018. V. 738. P. 13–24.

5. *Carlet C.* Boolean Functions for Cryptography and Coding Theory. Cambridge: Cambridge University Press, 2021.
6. *Siegenthaler T.* Correlation-immunity of nonlinear combining functions for cryptographic applications // IEEE Trans. Inform. Theory. 1984. V. 30. No. 5. P. 776–780.

УДК 519.7 DOI 10.17223/2226308X/15/10

О РАЗЛОЖЕНИИ БЕНТ-ФУНКЦИЙ ОТ ВОСЬМИ ПЕРЕМЕННЫХ В СУММУ ДВУХ БЕНТ-ФУНКЦИЙ[1]

А. С. Шапоренко

Максимально нелинейная булева функция от чётного числа переменных называется бент-функцией. Исследуется гипотеза о представлении произвольных булевых функций от n переменных степени не больше $n/2$ как суммы двух бент-функций. Доказано, что произвольная бент-функция от восьми переменных степени не больше 3 представляется как сумма двух бент-функций. Показано, что каждая квадратичная булева функция от чётного числа переменных $n \geqslant 4$ раскладывается в сумму двух бент-функций специального вида.

Ключевые слова: *бент-функции, булевы функции, разложение в сумму бент-функций.*

Булева функция $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ от чётного числа переменных n называется *бент-функцией*, если она находится на максимальном расстоянии Хэмминга от множества всех аффинных функций [1]. Обозначим через $\mathcal{B}_n$ множество бент-функций. Дальше полагаем, что n является чётным целым числом.

Преобразованием Уолша — Адамара булевой функции f от n переменных называется целочисленная функция, заданная на множестве $\mathbb{Z}_2^n$ равенством

$$W_f(y) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{f(x) \oplus \langle x,y \rangle} \text{ для любого } y \in \mathbb{Z}_2^n.$$

Для любой бент-функции f от n переменных $W_f(y) = \pm 2^{n/2}$ [2]. Определим *дуальную бент-функцию* $\tilde{f}$ к $f \in \mathcal{B}_n$ равенством $W_f(y) = 2^{n/2}(-1)^{\tilde{f}(y)}$ для любого $y \in \mathbb{Z}_2^n$.

Шифры, в которых используются бент-функции, более устойчивы к линейному криптоанализу [3], потому что бент-функции крайне плохо аппроксимируются аффинными функциями. Бент-функции используются в структуре блочного шифра CAST как координатные функции S-блоков [4], а также для построения регистра сдвига с нелинейной обратной связью в поточном шифре Grain [5]. Бент-функции связаны также с некоторыми объектами теории кодирования, например с кодами Рида — Маллера [2].

В работе исследуется известная открытая проблема о разложении произвольной булевой функции в сумму двух бент-функций [6].

Гипотеза 1 (Н. Н. Токарева, [7]). Любая булева функция от n переменных степени не больше $n/2$ может быть представлена как сумма двух бент-функций от n переменных.

В [7] показано, что гипотеза 1 верна для $n \leqslant 6$. Известно, что если гипотеза 1 верна, то справедлива следующая нижняя оценка числа бент-функций [7]:

$$|\mathcal{B}_n| \geqslant 2^{2^{n-2} + \binom{n}{n/2}/4}.$$

[1]Работа выполнена в рамках госзадания ИМ СО РАН (проект № FWNF-2022-0018).