УДК 510.644

А. В. СОКОЛОВ, О. Н. ЖДАНОВ, О. А. А ЙВАЗЯН

МЕТОДЫ СИНТЕЗА АЛГЕБРАИЧЕСКОЙ НОРМАЛЬНОЙ ФОРМЫ ФУНКЦИЙ МНОГОЗНАЧНОЙ ЛОГИКИ

[1]Одесский национальный политехнический университет, Одесса, Украина
[2]Сибирский государственный аэрокосмический университет им. академика М. Ф. Решетнева

Стремительное развитие методов помехоустойчивого кодирования, криптографии, теории синтеза сигналов, основанных на принципах многозначной логики, диктуют необходимость более полного изучения форм представления функций многозначной логики. В частности, для булевых функций широкое распространение получила алгебраическая нормальная форма, известная также как полином Жегалкина, которая хорошо описывает многие криптографические свойства булевых функций. В настоящей статье формализуется понятие алгебраической нормальной формы функции многозначной логики. Предложены методы синтеза алгебраической нормальной формы 3-функций и 5-функций, которые работают по аналогии с преобразованием Рида-Маллера для булевых функций: на основе рекуррентно синтезируемых матриц преобразования. Выдвинута гипотеза, определяющая правила синтеза матриц как для перехода от таблицы истинности к коэффициентам алгебраической нормальной формы, так и обратного преобразования для любого, наперед заданного количества переменных 3-функции либо 5-функции. В статье также введено определение алгебраической степени нелинейности функций многозначной логики и S-блока подстановки, основанных на принципах многозначной логики. Так, разработанный метод синтеза алгебраической нормальной формы 3-функций применен к известной конструкции рекуррентного синтеза S-блоков длины $N = 3^k$, в результате чего вычислены их алгебраические степени нелинейности. Полученные результаты могут стать основой как для дальнейших теоретических исследований, так и для практического применения: разработки новых криптографических примитивов, корректирующих кодов, алгоритмов сжатия информации, сигнальных конструкций, алгоритмов блочного и поточного шифрования, основанных на перспективных принципах многозначной логики. Кроме того, методы синтеза алгебраической нормальной формы функций многозначной логики являются основой для их программной и аппаратной имплементации.

Ключевые слова: *алгебраическая нормальная форма, многозначная логика, преобразование Рида-Маллера.*

Введение

Современный этап развития информационных технологий характеризуется активным исследованием свойств и внедрением принципов многозначной логики. То обстоятельство, что многозначная логика допускает более двух ($q > 2$) истинностных значений для высказываний, делает её привлекательной для создания корректирующих кодов, криптографических алгоритмов, алгоритмов сжатия информации, а также для построения систем сигналов. Так, в работах [1, 2] изучено применение q-ичных ортогональных преобразований для технологии CDMA, в работе [3] изучаются свойства корректирующих кодов, работы [4, 5] посвящены разработке методов синтеза сигнальных конструкций, основанных на принципах многозначной логики.

В работе [6] заложены основы конструирования криптографических примитивов на базе многозначной логики, в рамках чего предложен метод построения оптимальных троичных криптографических S-блоков подстановки длины 3^k, $k \in \mathbb{N}$.

Тем не менее, развитие методов телекоммуникационных технологий, основанных на возможностях многозначной логики, все еще находится на начальном этапе, что делает актуальной как с практической, так и с теоретической точки зрения задачу изучения форм представления функций многозначной логики или, кратко, q-функций.

Важнейшим инструментом, положенным в основу многих методов оценки криптографических свойств булевых функций, является полином Жегалкина, или алгебраическая нор-

мальная форма (АНФ). Так, с помощью АНФ оценивается алгебраическая степень нелинейности *S*-блоков подстановки, вводится понятие расстояния нелинейности [7]. На основе АНФ булевых функций предложен метод построения таких совершенных алгебраических конструкций, как бент-функции [8], которые играют существенную роль в теории кодирования и криптографии. АНФ также является основой построения важных в теории кодирования корректирующих кодов Рида-Маллера [9].

Отметим также, что АНФ булевых функций важны для реализации программируемых логических интегральных схем (ПЛИС). Еще одним применением АНФ является построение генераторов псевдослучайных ключевых последовательностей [10].

Из перечисленного уже ясна актуальность построения методов синтеза АНФ произвольной *q*-функции.

С другой стороны, быстрые методы нахождения АНФ, как и точное определение АНФ введено в литературе только для булевых функций, что ограничивает дальнейшее развитие теории и практики использования принципов многозначной логики в телекоммуникационных системах.

Целью настоящей статьи является разработка методов синтеза АНФ 3-функций и 5-функций.

1. Методы синтеза АНФ булевых функций

Способ представления булевых функций с помощью АНФ был предложен в 1927 году российским исследователем Иваном Жегалкиным [11] и с тех пор получил значительное распространение, связанное со многими свойствами, которые следуют из данной формы представления.

Определение 1 [12]. Полиномом Жегалкина называется полином над Z_2 с коэффициентами $a_i \in \{0,1\}$, содержащий операции «Исключающее ИЛИ» и «Конъюнкция».

Жегалкиным была доказана теорема: каждая булева функция может быть единственным образом представлена в виде АНФ.

Полином Жегалкина, состоящий из $N = 2^k$ термов, в общем виде может быть легко записан для булевых функций k переменных при любом, наперед заданном, значении k. Например, для булевых функций четырех переменных общий вид АНФ может быть представлен следующим образом:

$$\begin{aligned} f_i(x_1,x_2,x_3,x_4) = \sum_{i=0}^{N-1} a_i T_i = a_0 + a_4x_4 + a_3x_3 + \\ + a_{34}x_3x_4 + a_2x_2 + a_{24}x_2x_4 + a_{23}x_2x_3 + \\ + a_{234}x_2x_3x_4 + a_1x_1 + a_{14}x_1x_4 + a_{13}x_1x_3 + \\ + a_{134}x_1x_3x_4 + a_{12}x_1x_2 + x_{124}x_1x_2x_4 + \\ + a_{123}x_1x_2x_3 + a_{1234}x_1x_2x_3x_4, \end{aligned} \quad (1)$$

где коэффициенты $a_i \in \{0,1\}$ являются различными для различных булевых функций.

Задача поиска АНФ конкретной булевой функции сводится к нахождению значений коэффициентов $A = \{a_i\}$. Для решения данной задачи в литературе предложено достаточно большое количество методов, например, метод на основе карт Карно, метод треугольника, метод Паскаля и другие. Тем не менее, с вычислительной точки зрения, наиболее привлекательным является преобразование Рида-Маллера [12], позволяющие получить все коэффициенты АНФ путем умножения таблицы истинности булевой функции на матрицу Рида-Маллера L, которая строится в соответствии с рекуррентным правилом

$$L_1 = [1], \quad L_{2n} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \otimes L_n = \begin{bmatrix} L_n & L_n \\ 0 & L_n \end{bmatrix}, \quad (2)$$

где $\otimes$ – знак произведения Кронекера.

Матрица L обладает тем свойством, что над алфавитом $\{0,1\}$ для любого ее порядка выполняется равенство $L^{-1} = L$.

С учетом (2) для булевой функций k переменных могут быть легко найдены все коэффициенты её АНФ путем умножения матрицы преобразования порядка $N = 2^k$ на таблицу истинности булевой функции f. Естественным является и обратное преобразование

$$A = fL_n, \quad f = AL_n, \quad (3)$$

Таким образом, (3) полностью определяет прямое и обратное преобразование Рида-Маллера, позволяющее путем простого матричного умножения получить коэффициенты АНФ произвольной булевой функции.

2. Метод синтеза АНФ 3-функций

Аппарат алгебраической нормальной формы булевых функций, являющийся мощным инструментом их исследования и практического использования, может быть расширен на

q-функции, которые получили существенное распространение в современных информационных технологиях.

Определение 2 [6]. Функцией q-значной логики k переменных называется отображение $\{0,1,2,...,q-1\}^k \to \{0,1,2,...,q-1\}$, q – простое. При $q=2$ получаем булевы функции.

Функция трехзначной логики (3-функция) – это отображение $\{0,1,2\}^k \to \{0,1,2\}$, т. е. правило, однозначно сопоставляющее вектору из k координат, принимающих значения 0, 1, 2 значение 0,1 или 2.

Аналогично полиномам Жегалкина для случая булевых функций мы вводим определение алгебраической нормальной формы q-функций.

Определение 3. Алгебраической нормальной формой q-функции называется полином Ф над Z_q степени $\deg(\Phi) < q$ с коэффициентами $a_i \in \{0,1,...,q-1\}$, содержащий операции «Сумма по модулю q» и «Умножение по модулю q».

Пример. Рассмотрим 3-функции $k=2$ переменных, таблица истинности которых имеет длину $N=9$ и может быть представлена в общем виде

$$f = \{f_{00}, f_{01}, f_{02}, f_{10}, f_{11}, f_{12}, f_{20}, f_{21}, f_{22}\}. \quad (4)$$

С другой стороны, в соответствии с Определением 2 для 3-функций двух переменных можно выписать полином АНФ в общем виде

$$f(x_1,x_2) = a_{00} + a_{01}x_2 + a_{02}x_2^{\,2} + a_{10}x_1 + a_{11}x_1x_2 + a_{12}x_1x_2^{\,2} + a_{20}x_1^{\,2} + a_{21}x_1^{\,2}x_2 + a_{22}x_1^{\,2}x_2^{\,2}, \quad (5)$$

где $a_{ij} \in \{0,1,2\}$ – искомые коэффициенты.

Для того чтобы связать искомые коэффициенты a_{ij} с элементами таблицы истинности 3-функции (4), записываем соответствующую систему уравнений

$$\begin{cases} f_{00} = a_{00}; \\ f_{01} = a_{00} + a_{01} + a_{02}; \\ f_{02} = a_{00} + 2a_{01} + a_{02}; \\ f_{10} = a_{00} + a_{10} + a_{20}; \\ f_{11} = a_{00} + a_{01} + a_{10} + a_{02} + a_{11} + a_{20} + a_{12} + a_{21} + a_{22}; \\ f_{12} = a_{00} + 2a_{01} + a_{10} + a_{02} + 2a_{11} + a_{20} + a_{12} + \\ \quad + 2a_{21} + a_{22}; \\ f_{20} = a_{00} + 2a_{10} + a_{20}; \\ f_{21} = a_{00} + a_{01} + 2a_{10} + a_{02} + 2a_{11} + a_{20} + 2a_{12} + \\ \quad + a_{21} + a_{22}; \\ f_{22} = a_{00} + 2a_{01} + 2a_{10} + a_{02} + a_{11} + a_{20} + 2a_{12} + \\ \quad + 2a_{21} + a_{22}, \end{cases} \quad (6)$$

где знак «+» следует понимать как сложение по модулю 3.

Представляя найденную систему уравнений в матричной форме, получаем, соответственно, матрицу L_9^{-1} для случая 3-функций двух переменных

$$L_9^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 & 2 & 1 & 1 & 2 & 1 \\ 1 & 0 & 0 & 2 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 2 & 2 & 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 \end{bmatrix}. \quad (7)$$

Проведенные эмпирические исследования позволили выдвинуть гипотезу: построение матриц обратного преобразования АНФ L_n^{-1} порядка n, кратного трем, может быть осуществлено в соответствии со следующей рекуррентной формулой

$$L_{3n}^{-1} = \begin{bmatrix} L_n^{-1} & 0 & 0 \\ L_n^{-1} & L_n^{-1} & L_n^{-1} \\ L_n^{-1} & 2L_n^{-1} & L_n^{-1} \end{bmatrix}, \; L_1^{-1} = [1], \quad (8)$$

где по знаком «0» понимается нулевая матрица порядка n.

Вычислительные эксперименты, проведенные в среде Matlab, позволили подтвердить правильность выдвинутой гипотезы для практически ценных значений $n < 6$. Тем не менее, аналитическое доказательство (8) может представлять математический интерес, и являться предметом дальнейших исследований.

Для нахождения матрицы прямого преобразования (необходимой для расчета коэффициентов АНФ) матрица L_n^{-1} должна быть обращена

$$L = (L^{-1})^{-1} = \mathrm{adj}(L) \cdot \det^{-1}(L), \quad (9)$$

где $\mathrm{adj}(L)$ – союзная матрица над алфавитом $\{0,1,2\}$, $\det^{-1}(L)$ – элемент, обратный к определителю матрицы L.

Для матрицы (7), т. е. для случая 3-функций двух переменных обратная матрица имеет следующий вид

$$L_9 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 2 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}. \quad (10)$$

Отметим важное свойство: в отличие от случая булевых функций, для q-функций при $q > 2$ матрицы прямого и обратного преобразования АНФ не совпадают.

Основываясь на (7), (8) и (9), можем записать регулярный метод нахождения АНФ 3-функций произвольного количества переменных в виде шагов.

Шаг 1. Основываясь на (8) с учетом (7) найти матрицу обратного преобразования L_n^{-1} необходимого порядка $n = 3^k$.

Шаг 2. На основе (9) либо же с использованием одного из известных алгоритмов обращения матриц над алфавитом $\{0,1,...,q-1\}$ [13] найти матрицу L.

Шаг 3. В соответствии с (3) вычислить искомые коэффициенты АНФ.

Рассмотрим пример, иллюстрирующий работу предложенного метода. Пусть, например, задана 3-функция пяти переменных в виде своей таблицы истинности

$$\begin{array}{l} f = \{00022211100022211100022211100022 \\ 21110002221110002221110002221110022 \\ 21110002221110002221110002221110022 \\ 21111110002221110202211101022011100 \\ 02221110012021110022120002221110022 \\ 21110002221112221110002221100202221 1 \\ \quad 20102221110002221210012221010 02\}. \end{array} \quad (11)$$

Путем умножения таблицы истинности булевой функции (11) на матрицу L_{243}, построенную в соответствии с (8), получаем коэффициенты АНФ интересующей нас 3-функции

$$\begin{array}{l} A = \{00020000000000000000000000000000 \\ 00000000000000000000000000000000000 \\ 00000000000000000000000000000000000 \\ 00000000000000000000000000000010000 \\ 00000000100000000000000000000000000 \\ 00000000000000000000000000000100000 \\ \quad 00000000000000000000000000000000\}, \end{array} \quad (12)$$

а также, собственно, АНФ

$$\Phi(x_1,x_2,x_3,x_4,x_5) = 2x_4 + x_1x_2^{\,2} + \\ + x_1x_2^{\,2}x_3x_4x_5 + x_1^{\,2}x_2x_3x_4^{\,2}x_5^{\,2}. \quad (13)$$

Подстановка значений $\{x_1,x_2,x_3,x_4,x_5\}$ в (13) позволяет снова вернуться к таблице истинности (11), что подтверждает правильность полученной АНФ.

Отметим, что подобно преобразованию Рида-Маллера (3), применение разработанного регулярного метода нахождения АНФ 3-функций по вычислительной сложности эквивалентно умножению матрицы на вектор, при условии, что матрица преобразования найдена заблаговременно. Данное свойство предложенного метода обуславливает его высокую практическую ценность.

3. Метод синтеза АНФ 5-функций

Аналогичным образом могут быть найдены матрицы преобразования L^{-1} и L для случая 5-функций. Эмпирические исследования позволили сформулировать гипотезу: матрицы L^{-1} для 5-функции любого числа переменных могут быть найдены с помощью следующей рекуррентной формулы

$$L_{5n}^{-1} = \begin{bmatrix} L_n^{-1} & 0 & 0 & 0 & 0 \\ L_n^{-1} & L_n^{-1} & L_n^{-1} & L_n^{-1} & L_n^{-1} \\ L_n^{-1} & 2L_n^{-1} & 4L_n^{-1} & 3L_n^{-1} & L_n^{-1} \\ L_n^{-1} & 3L_n^{-1} & 4L_n^{-1} & 2L_n^{-1} & L_n^{-1} \\ L_n^{-1} & 4L_n^{-1} & L_n^{-1} & 4L_n^{-1} & L_n^{-1} \end{bmatrix},$$

$$L_1^{-1} = [1], \quad (14)$$

где под знаком «0» понимается нулевая матрица порядка n.

Для обращения матриц над конечными полями существуют хорошо разработанные методы, см., например, [13].

В качестве примера приведем матрицы L_{25}^{-1} и L_{25} соответственно.

$$L_{25}^{-1} = \begin{bmatrix} 10000000000000000000000000 \\ 11111000000000000000000000 \\ 12431000000000000000000000 \\ 13421000000000000000000000 \\ 14141000000000000000000000 \\ 10000100001000010000100000 \\ 11111111111111111111111111 \\ 12431124311243112431124311 \\ 13421134211342113421134211 \\ 14141141411414114141141411 \\ 10000200004000030000100000 \\ 11111222224444433333111111 \\ 12431243124312431243124311 \\ 13421213424213434213134211 \\ 14141232324141432323141411 \\ 10000300004000020000100000 \\ 11111333334444422222111111 \\ 12431312434312424312124311 \\ 13421342134213421342134211 \\ 14141323234141423232141411 \\ 10000400001000040000100000 \\ 11111444441111144444111111 \\ 12431431241243143124124311 \\ 13421421341342142134134211 \\ 14141414141414141414141411 \end{bmatrix},$$

$$L_{25}=\begin{bmatrix}
10000000000000000000000000\\
04231000000000000000000000\\
04114000000000000000000000\\
04321000000000000000000000\\
44444000000000000000000000\\
00004000020000300001000 0\\
00000132403412021430423 1\\
00000144103223023320411 4\\
00000123403142024130432 1\\
00001111133333222244444\\
00004000010000100004000 0\\
00000132404231042310132 4\\
00000144104114041140144 1\\
00000123404321043210123 4\\
00001111144444444441111 1\\
00004000030000200001000 0\\
00000132402143034120423 1\\
00000144102332032230411 4\\
00000123402413031420432 1\\
00001111122222333344444\\
40004000040000400004000 0\\
01324013240132401324013 4\\
01441014410144101441014 1\\
01234012340123401234012 4\\
11111111111111111111111 1
\end{bmatrix} \quad (15)$$

Обобщая метод, разработанный ранее для 3-функций, приведем пример, иллюстрирующий полученные результаты для 5-функций. Пусть 5-функция трех переменных задана своей таблицей истинности

$$\begin{aligned}f=\{&01234043210314203142043211234014\\&40213134144311230340123432444021241 1\\&32414044012344410412134102244342123 4\\&0102331341411433142 40\}.\end{aligned} \quad (16)$$

Путем умножения таблицы истинности 5-функции (16) на матрицу L_{125} получаем коэффициенты АНФ

$$\begin{aligned}A=\{&01000000000300000000000000000000\\&00400000000000000010000020000000000 0\\&00000000000000000003000000000000000 0\\&00000000000000000000\},\end{aligned} \quad (17)$$

и теперь легко выписать АНФ рассматриваемой 5-функции

$$\begin{aligned}\Phi(x_1,x_2,x_3)=x_3+3{x_2}^2x_3+4x_1x_2{x_3}^4+\\+{x_1}^2+2{x_1}^2x_2x_3+3{x_1}^3{x_2}^2{x_3}^2.\end{aligned} \quad (18)$$

Непосредственными вычислениями значений $\Phi(x_1,x_2,x_3)$ легко проверить правильность полученной формулы.

4. Некоторые практические приложения разработанных методов

В качестве примера работы предложенных методов синтеза АНФ функций многозначной логики исследуем алгебраическую степень нелинейности, предложенных в [6] оптимальных троичных *S*-блоков подстановки. Так, рассмотрим оптимальный *S*-блок длины $N=27$

$$\begin{aligned}S_{27}=\{&0,2,24,26,25,14,13,12,1,9,11,6,8,7,23,\\&22,21,10,18,20,15,17,16,5,4,3,19\},\end{aligned} \quad (19)$$

который можно представить в виде трех 3-функций трех переменных

$$\begin{cases}f_1=\{00222111011000222122111 0002\};\\ f_2=\{00222111000222111000222111 0\};\\ f_3=\{02021210102021210102021210 1\},\end{cases} \quad (20)$$

для каждой из которых, зная соответствующую матрицу L_{27}, нетрудно найти АНФ

$$\begin{cases}\Phi_1(x_1,x_2,x_3)=2x_3+{x_3}^2+2x_2+x_1;\\ \Phi_2(x_1,x_2,x_3)=2x_3+{x_3}^2+2x_2;\\ \Phi_3(x_1,x_2,x_3)=x_3+{x_3}^2+2x_2.\end{cases} \quad (21)$$

Для нахождения алгебраической степени нелинейности S-блока подстановки (19) воспользуемся определением [7].

Определение 4 [7]. Алгебраической степенью нелинейности функции (обозначение: $\deg(f)$) называется степень слагаемого в полиноме АНФ, содержащего наибольшее число переменных.

Определение 5 [14]. Алгебраическая степень нелинейности *S*-блока подстановки определяется как минимум среди алгебраических степеней его компонентных функций.

Таким образом, с учетом (21) нетрудно установить, что алгебраическая степень нелинейности *S*-блока подстановки (19) $\deg(S_{27})=2$.

Проведенные выборочные исследования *S*-блоков подстановки, генерируемых с помощью метода рекуррентного увеличения длины [6], позволили установить, что алгебраическая степень нелинейности *S*-блоков подстановки не возрастает при увеличении их длины с помощью метода [6].

Задача изучения алгебраических степеней нелинейности подстановочных конструкций, основанных на принципах многозначной логики и задача синтеза оптимальных, с точки зрения максимизации алгебраической степени нелинейности *S*-блоков подстановки, все еще ожидают своего решения.

Заключение

1. Предложены методы синтеза алгебраической нормальной формы 3-функций и 5-функций допускающие нахождение коэффициентов

АНФ для q-функции любой длины. При этом, определено обратное преобразование, позволяющее получить таблицу истинности 3-функций или 5-функций при наличии вектора коэффициентов АНФ. Сложность предложенных методов практически эквивалентна сложности операции умножения матрицы на вектор.

2. Рассчитаны АНФ компонентных 3-функций оптимальных S-блоков подстановки. Установлено, что недостатком метода рекуррентного увеличения длины оптимальных S-блоков подстановки является тот факт, что с увеличением длины их алгебраическая степень нелинейности не возрастает.

3. Предложенные методы синтеза АНФ могут быть использованы как для тестирования криптографических примитивов или построения корректирующих кодов, так и для аппаратной или программной реализации 3-функций и 5-функций.

Литература

1. **Мазурков, М. И.** О влиянии вида ортогонального преобразования на пик-фактор спектра в системах с CDMA / М. И. Мазурков, А. В. Соколов, Н. А. Барабанов. – Інформатика та математичні методи в моделюванні, 2015. – Т .5, № 1. – С. 28–37.

2. **Falkowski, B. J.** Application of Sign Hadamard-Haar Transform in Ternary Communication System / B. J. Falkowski, S. Yan. – International Journal of Electronics, 1995. – Vol. 79(5). – P. 551–559.

3. **Кузнецов, В. С.** Троичные каскадные коды с модуляцией КАМ-9 и их возможности / В. С. Кузнецов. – «Инфо-Электросвязь», 2009. – С. 30–33.

4. **Мазурков, М. И.** Системы широкополосной радиосвязи / М. И. Мазурков – Одесса: Наука и Техника, 2010, с. 340. – ISBN 978-966-8335-95-2.

5. **Петелин, Ю. В.** Перспективы использования сигнально-кодовых конструкций типа троичных М-последовательностей в спутниковых каналах связи / Ю. В. Петелин, М. А. Ковалев, А. А. Макаров // Информационно-управляющие системы. – 2006. – №. 5. – С. 32–35.

6. **Жданов, О. Н.** Алгоритм построения оптимальных по критерию нулевой корреляции недвоичных блоков замен / О. Н. Жданов, А. В. Соколов. – Проблемы физики, математики и техники, 2015. – № 3(24). – С. 94–97.

7. **Логачев, О. А.** Булевы функции в теории кодирования и криптологии / О. А. Логачев, А. А. Сальников, В. В. Ященко. – М: Издательство МЦНМО. – 2004. – 472 с.

8. **Qingshu, Meng** A novel algorithm enumerating bent functions / Qingshu Meng, Min Yang, Huanguo Zhang, Jingsong Cui // Discrete Mathematics, 2008. – Volume 308, Issue 23, 2008. – P. 5576–5584.

9. **Мак-Вильямс, Ф. Дж.** Теория кодов исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. – М.: Связь, 1979. – с. 745.

10. **Мазурков, М. И.** Генератор ключевых последовательностей на основе дуальных пар бент-функций / М. И. Мазурков, Н. А. Барабанов, А. В. Соколов. – Труды Одесского политехнического университета, 2013. – Вып. 3 (42). – С. 150–156.

11. **Жегалкин, И. И.** Арифметизация символической логики / И. И. Жегалкин. – Матем. сб., 1929. – 305–338.

12. **Ростовцев, А. Г.** Криптография и защита информации / А. Г. Ростовцев. – СПб.: Мир и Семья. – 2002.

13. **Кормен, Т.** Алгоритмы: построение и анализ / Т. Кормен, Ч. Лейзерсон, Р. Ривест, К. Штайн, – М.: Вильямс, 2006. – с. 1328.

14. **Соколов, А. В.** Новые методы синтеза нелинейных преобразований современных шифров / А. В. Соколов. – Lap Lambert Academic Publishing, Germany, 2015. – 100 с.

References

1. **Mazurkov, M. I.** On the effect of the type of orthogonal transform on PAPR of signal spectrum in CDMA systems / M. I. Mazurkov, A. V. Sokolov, N. A. Barabanov. – Informatika ta matematichni metodi v modeljuvanni, 2015. – Vol. 5, № 1. – P. 28–37.

2. **Falkowski, B. J.** Application of Sign Hadamard-Haar Transform in Ternary Communication System / B. J. Falkowski, S. Yan. – International Journal of Electronics, 1995. – Vol. 79(5). – P. 551–559.

3. **Kuznecov, V. S.** Trinity concatenated codes with QAM-9 and their capabilities / V. S. Kuznecov. – «Info-Jelektrosvjaz», 2009. – P. 30–33.

4. **Mazurkov, M. I.** Broadband radio systems / M. I. Mazurkov. – Odessa: Nauka i Tehnika, 2010, p. 340. – ISBN 978-966-8335-95-2.

5. **Petelin, Ju. V.** Perspectives of using of signal-code structures such as ternary M-sequences in the satellite communication channels / Ju. V. Petelin, M. A. Kovalev, A. A. Makarov // Informacionno-upravljajushhie sistemy. – 2006. – №. 5. – P. 32–35.

6. **Zhdanov, O. N.** Algorithm of construction of optimal according to criterion of zero correlation nonbinary S-boxes / O. N. Zhdanov, A. V. Sokolov. – Problems of physics, mathematics and technics, 2015. – № 3(24). – P. 94–97.

7. **Logachev, O. A.** Boolean functions in coding theory and cryptology / O. A. Logachev, A. A. Sal'nikov, V. V. Jashhenko. – M: Izdatel'stvo MCNMO. – 2004. – 472 p.

8. **Qingshu, Meng** A novel algorithm enumerating bent functions / Qingshu Meng, Min Yang, Huanguo Zhang, Jingsong Cui // Discrete Mathematics, 2008. – Volume 308, Issue 23. – P. 5576–5584.

9. **MacWilliams, F. J.** Theory of Error-Correcting Codes / F. J. MacWilliams, N. J. A. Sloane. – M.: Svjaz', 1979. – p. 745.

10. **Mazurkov, M. I.** The key sequences generator based on bent functions dual couples / M. I. Mazurkov, N. A. Barabanov, A. V. Sokolov. – Works of the Odessa polytechnic university. – Vol. 3 (42). – P. 150–156.

11. **Zhegalkin, I. I.** Arithmetization of symbolic logic / I. I. Zhegalkin. – Matem. sb., 1929. – P. 305–338.

12. **Rostovcev, A. G.** Cryptography and Data Protection / A. G. Rostovcev. – SPb.: Mir i Sem'ja. – 2002.

13. **Kormen, T.** Construction and analysis of algorithms / T. Kormen, Ch. Lejzerson, R. Rivest, K. Shtajn, – M.: Vil'jams, 2006. – p. 1328.

14. **Sokolov, A. V.** New methods of the synthesis of non-linear transforms of modern ciphers / A. V. Sokolov. – Lap Lambert Academic Publishing, Germany, 2015. – p. 100.

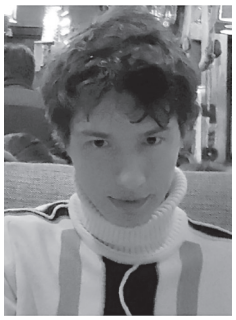
Поступила 01.03.2016

A. V. Sokolov, O. N. Zhdanov, O. A. Ayvazian

SYNTHESIS METHODS OF ALGEBRAIC NORMAL FORM OF MANY-VALUED LOGIC FUNCTIONS

The rapid development of methods of error-correcting coding, cryptography, and signal synthesis theory based on the principles of many-valued logic determines the need for a more detailed study of the forms of representation of functions of many-valued logic. In particular the algebraic normal form of Boolean functions, also known as Zhegalkin polynomial, that well describe many of the cryptographic properties of Boolean functions is widely used. In this article, we formalized the notion of algebraic normal form for many-valued logic functions. We developed a fast method of synthesis of algebraic normal form of 3-functions and 5-functions that work similarly to the Reed-Muller transform for Boolean functions: on the basis of recurrently synthesized transform matrices. We propose the hypothesis, which determines the rules of the synthesis of these matrices for the transformation from the truth table to the coefficients of the algebraic normal form and the inverse transform for any given number of variables of 3-functions or 5-functions. The article also introduces the definition of algebraic degree of nonlinearity of the functions of many-valued logic and the S-box, based on the principles of many-valued logic. Thus, the methods of synthesis of algebraic normal form of 3-functions applied to the known construction of recurrent synthesis of S-boxes of length $N = 3^k$, whereby their algebraic degrees of nonlinearity are computed. The results could be the basis for further theoretical research and practical applications such as: the development of new cryptographic primitives, error-correcting codes, algorithms of data compression, signal structures, and algorithms of block and stream encryption, all based on the perspective principles of many-valued logic. In addition, the fast method of synthesis of algebraic normal form of many-valued logic functions is the basis for their software and hardware implementation.

Keywords: *algebraic normal form, many-valued logic, Reed-Muller transform.*



Артем Соколов родился 15 апреля 1990 года в Одессе, УССР. Получил степень бакалавра (с отличием) по специальности «Системы технической защиты информации» в 2011 году, степень магистра (с отличием) по специальности «Системы технической защиты информации, автоматизация её обработки» в 2013 году и степень кандидата технических наук по специальности «Системы защиты информации» в 2014 году в Одесском национальном политехническом университете, г. Одесса, Украина.

С 2012 по 2014 работал младшим научным сотрудником кафедры Информационной безопасности в Одесском национальном политехническом университете. С 2014 года является старшим преподавателем кафедры Информационной безопасности Одесского национального политехнического университета. Является автором монографии и более 30 научных статей. Научные интересы включают в себя методы защиты информации на основе совершенных алгебраических конструкций, методы синтеза алгоритмов шифрования данных и нелинейных S-блоков.

Артем Соколов награжден Золотой медалью за высокие достижения в учебе, Дипломом победителя в конкурсе Магистров, 2013 год; Дипломом победителя Всеукраинского конкурса научно-исследовательских работ «Телекоммуникационные системы и сети», 2012 год; Дипломом за высокие академические и исследовательские достижения, 2010 год.

Жданов Олег Николаевич родился 16 апреля 1964 года. В 1986 году окончил Красноярский Государственный Университет. Кандидатская диссертация по специальности «математический анализ» защищена в 1994 году. В настоящее время доцент кафедры безопасности информационных технологий Сибирского Государственного Аэрокосмического университета.

Читаемые лекционные курсы: «Криптографические методы защиты информации» (имеется удостоверение Института Криптографии, Связи и Информатики о соответствующем повышении квалификации), «Теоретико-числовые алгоритмы криптографии», «Теория надежности».

Общее количество публикаций 73, из них 7 – учебные пособия (в соавторстве с учениками).

Сфера научных интересов: системы дифференциальных уравнений в частных производных, являющиеся моделями процессов в механике сплошных сред. Получены точные решения уравнений пластичности плоского напряженного состояния, предложен новый подход к исследованию смешанной задачи для системы уравнений плоского напряженного состояния среды Мизеса, построен алгоритм нахождения решения задачи Коши для системы уравнений, описывающей одномерный поток гранулированного материала.

Еще одной областью научных интересов является защита информации: разработка реализации алгоритмов шифрования данных при передаче по открытому каналу с привлечением к этой работе студентов старших курсов для выполнения ими курсового и дипломного проектирования. Совместно с учениками разработал методику выбора ключевой информации для реализации алгоритмов блочного шифрования. Получено авторское свидетельство (совместно с Чалкиным Т. А.) на программный комплекс, реализующий выбор ключевой информации для шифрования данных по действующему стандарту России.

Два ученика стали лауреатами стипендии губернатора Красноярского края, а один – лауреат стипендии Правительства России и победитель конкурса на лучшую студенческую научную работу.

Награжден Благодарственным Письмом Законодательного Собрания Красноярского края. Награжден нагрудным знаком Министерства Образования и Науки РФ «За развитие научно-исследовательской работы студентов».

Айвазян Оганнес родился в Ереване, АССР, в 1990 году. Получил степень бакалавра по специальности «Компьютерные науки» в 2011 году, степень специалиста по специальности «Информационные системы проектирования» в 2012 году в Одесском национальном политехническом университете, г. Одесса, Украина.

С ноября 2013 года является аспирантом по специальности «Компьютерные системы и компоненты» и работает инженером-программистом. Научные интересы включают в себя методы недвоичного обнаружения и исправления ошибок, методы сглаживания и экстраполяции данных, квантовая обработка информации.

Айвазян Оганнес награжден грамотами за призовые места на олимпиадах.