УДК 510.644

Соколов А.В., Оверчук Ю.С.
Одесский национальный политехнический университет,
radiosquid@gmail.com

О ВОЗМОЖНОСТИ СИНТЕЗА АЛГЕБРАИЧЕСКОЙ НОРМАЛЬНОЙ ФОРМЫ ЧЕТВЕРИЧНЫХ ФУНКЦИЙ НАД ПОЛЕМ $GF(4)$

Синтез и анализ современных криптографических алгоритмов основан на всеобъемлющем применении математического аппарата булевых функций. Именно свойствами булевых функций, входящих в состав криптоалгоритма, определяется его криптографическая стойкость и быстродействие. Важнейшим и наиболее распространенным сегодня способом представления булевых функций является их алгебраическая нормальная форма (АНФ) [1].

Способ представления булевых функций с помощью АНФ был предложен в 1927 году Иваном Жегалкиным [2] и с тех пор получил широкое распространение: АНФ булевых функций представляет значительное удобство в изучении их криптографических свойств.

Так, важнейшее, с криптографической точки зрения, свойство булевых функций — алгебраическая степень нелинейности, определено через степень АНФ. Алгебраическая степень нелинейности стала основой определения расстояния нелинейности и открытия таких совершенных алгебраических конструкций как бент-функции, которые столь широко используются в современной криптографии [3].

Определение 1 [1]. 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.

Новый этап в развитии информационных технологий, в частности, методов криптографической защиты информации характеризуется внедрением методов многозначной логики, что

ставит задачу исследования форм представления и свойств функций многозначной логики.

Описание конструкций многозначной логики также во многом опирается на такое базовое определение, как АНФ функций многозначной логики, методы синтеза которой для троичного и пятеричного случая были предложены в работе [4].

Отметим, тем не менее, что несмотря на бурное развитие математического аппарата функций многозначной логики, подавляющее большинство современных вычислительных устройств построены на основе двоичной логики, что приводит к существенным потерям в производительности при использовании алгоритмов многозначной логики. Компромиссом является использование конструкций полей $GF(2^k)$. Так, в работе [5] предложен метод оценки нелинейности 4-функций на основе четверичного преобразования Виленкина-Крестенсона. Тем не менее, математический аппарат синтеза АНФ 4-функций над полем $GF(4)$ на сегодня отсутствует, что не позволяет вычислять такой важный критерий криптографического качества, как алгебраическая степень нелинейности 4-функций.

Утверждение. Всякую 4-функцию можно единственным образом представить с помощью АНФ над полем $GF(4)$, т.е. с помощью полинома, содержащего операции сложения и умножения в поле $GF(4)$.

Данные операции описываются следующими таблицами

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

,

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

. (1)

Например, рассмотрим 4-функцию одной переменной x_1. В общем случае АНФ 4-функции одной переменной имеет вид

$$\Phi(x_1) = a_0 + a_1 x_1 + a_2 x_1^2 + a_3 x_1^3, \quad (2)$$

тогда как набор коэффициентов a_i определяется конкретно для каждой 4-функции одной переменной $f(x_1) = \{f_0 \ f_1 \ f_2 \ f_3\}$, представленной в виде таблицы истинности.

Следующая система уравнений связывает коэффициенты a_i с элементами таблицы истинности f_j

$$\begin{cases} f_0 = a_0; \\ f_1 = a_0 + a_1 + a_2 + a_3; \\ f_2 = a_0 + 2a_1 + 3a_1 + a_3; \\ f_3 = a_0 + 3a_1 + 2a_2 + a_3. \end{cases} \quad (3)$$

Систему уравнений (3) легко записать в матричной форме

$$F = L_4^{-1} A, \text{ где } F = \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \end{bmatrix}, \; A = \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}, \quad (4)$$

где $L_4^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 3 & 2 & 1 \end{bmatrix}$ — обратная матрица преобразования Рида-Маллера.

Для того, чтобы вычислить коэффициенты АНФ конкретно заданной 4-функции, удобно использовать следующее матричное уравнение

$$A = L_4 F,$$

где L_4 — матрица преобразования Рида-Маллера.

Для того, чтобы найти матрицу L_4, необходимо обратить матрицу L_4^{-1} над полем $GF(4)$. В нашем случае матрица L_4 будет иметь вид

$$L_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 3 & 2 \\ 0 & 1 & 2 & 3 \\ 1 & 1 & 1 & 1 \end{bmatrix}.$$

Аналогичным (2) образом может быть записан общий вид АНФ 4-функций двух переменных

$$\begin{aligned} \Phi(x_1, x_2) = a_0 + a_{01}x_2 + a_{02}x_2^2 + a_{03}x_2^3 + a_{10}x_1 + a_{11}x_1x_2 + \\ + a_{12}x_1x_2^2 + a_{13}x_1x_2^3 + a_{20}x_1^2 + a_{21}x_1^2x_2 + a_{22}x_1^2x_2^2 + \\ a_{23}x_1^2x_2^3 + a_{30}x_1^3 + a_{31}x_1^3x_2 + a_{32}x_1^3x_2^2 + a_{33}x_1^3x_2^3. \end{aligned} \quad (5)$$

Записывая систему уравнений и получая прямую и обратную матрицы преобразования Рида-Маллера для случая четверичных

функций двух переменных, нетрудно записать рекуррентные правила их формирования для четверичных функций произвольного числа переменных k

$$L_{4^k}^{-1}=\begin{bmatrix} L_{4^{k-1}}^{-1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ L_{4^{k-1}}^{-1} & L_{4^{k-1}}^{-1} & L_{4^{k-1}}^{-1} & L_{4^{k-1}}^{-1} \\ L_{4^{k-1}}^{-1} & 2L_{4^{k-1}}^{-1} & 3L_{4^{k-1}}^{-1} & L_{4^{k-1}}^{-1} \\ L_{4^{k-1}}^{-1} & 3L_{4^{k-1}}^{-1} & 2L_{4^{k-1}}^{-1} & L_{4^{k-1}}^{-1} \end{bmatrix},\ L_{4^k}=\begin{bmatrix} L_{4^{k-1}} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & L_{4^{k-1}} & 3L_{4^{k-1}} & 2L_{4^{k-1}} \\ \mathbf{0} & L_{4^{k-1}} & 2L_{4^{k-1}} & 3L_{4^{k-1}} \\ L_{4^{k-1}} & L_{4^{k-1}} & L_{4^{k-1}} & L_{4^{k-1}} \end{bmatrix},$$

где под $\mathbf{0}$ понимается нулевая матрица порядка 4^{k-1}.

Кратко обозначим результаты проведенных исследований:

1. Показана возможность представления функций четверичной логики с помощью АНФ над полем $GF(4)$. Установлена единственность такого представления.

2. Найден общей вид прямой и обратной матрицы преобразования Рида-Маллера для быстрого нахождения АНФ четверичных функций произвольного числа переменных k над полем $GF(4)$.

Литература

1. Ростовцев, А.Г. Криптография и защита информации / А.Г. Ростовцев. — СПб.: Мир и Семья. — 2002.

2. Жегалкин, И.И. Арифметизация символической логики / И.И. Жегалкин. — Матем. сб., 1929. — 305—338.

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

4. Соколов, А.В. Методы синтеза алгебраической нормальной формы функций многозначной логики / А.В. Соколов, О.Н. Жданов, А.О. Айвазян. — Системный анализ и прикладная информатика, 2016. — №1. — С. 69—76.

5. Соколов А.В. Сильно нелинейные подстановки: метод синтеза S-блоков, обладающих максимальной 4-нелинейностью / А.В. Соколов, Н.И. Красота. — Наукові праці ОНАЗ ім. О.С. Попова, 2017, № 1. — С. 145—154.