ЛИТЕРАТУРА

1. *Агибалов Г. П.* Методы решения систем полиномиальных уравнений над конечным полем // Вестник Томского государственного университета. Приложение. 2006. № 17. С. 4–9.
2. *Courtois N. and Meier W.* Algebraic attacks on stream ciphers with linear feedback // Eurocrypt 2003. LNCS. 2003. V. 2656. P. 345–359.
3. *Meier W., Pasalic E., and Carlet C.* Algebraic attacks and decomposition of Boolean functions // Eurocrypt 2004. LNCS. 2004. V. 3027. P. 474–491.
4. *Carlet C.* On the algebraic immunities and higher order nonlinearities of vectorial Boolean functions // Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes. Amsterdam: IOS Press, 2009. P. 104–116.
5. *Покрасенко Д. П.* О максимальной компонентной алгебраической иммунности векторных булевых функций // Дискретный анализ и исследование операций. 2016. Т. 23. № 2. С. 88–99.

УДК 512.13 DOI 10.17223/2226308X/10/22

СПОСОБ ПРЕДСТАВЛЕНИЯ ПОДСТАНОВОК S_{16} С ПОМОЩЬЮ АЛГЕБРАИЧЕСКИХ ПОРОГОВЫХ ФУНКЦИЙ

Д. А. Сошин

Предлагается алгоритм представления подстановок на множестве элементов $\{0, 1, \ldots, 15\}$ с помощью линейных комбинаций алгебраических пороговых функций. Получаемые задания могут быть использованы для эффективной реализации на перспективной оптической элементной базе нелинейных преобразований узлов переработки информации.

Ключевые слова: *алгебраические пороговые функции, геометрические типы, подстановки, блочные шифры.*

Определение 1. Функцию k-значной логики $f : \Omega_k^n \to \Omega_k$ назовём *алгебраической пороговой* (АПФ), если существуют целочисленные наборы $\mathbf{c} = (c_0, c_1, \ldots, c_n)$, $\mathbf{b} = (b_0, b_1, \ldots, b_k)$ и натуральный модуль m, такие, что для любого $\alpha \in \Omega_k$ выполняется

$$f(x_1, x_2, \ldots, x_n) = \alpha \quad \Leftrightarrow \quad b_\alpha \leqslant r_m(c_0 + c_1x_1 + c_2x_2 + \ldots + c_nx_n) < b_{\alpha+1},$$

где $r_m(x)$ — функция взятия остатка числа x по модулю m, $r_m(x) \in \{0, 1, \ldots, m-1\}$; $\Omega_k = \{0, 1, \ldots, k-1\}$. Тройку $(\mathbf{c}, \mathbf{b}, m)$ будем называть *структурой функции* f.

В случае двузначной логики АПФ будем задавать следующим образом:

$$f = 1 \quad \Leftrightarrow \quad r_m(c_0 + c_1x_1 + c_2x_2 + \cdots + c_nx_n) \geqslant b$$

и писать $f : ((c_0, c_1, c_2, \ldots, c_n); b; m)$.

В [1] исследован вопрос реализации булевых функций трёх переменных функциями из класса АПФ. Для этого доказана замкнутость данного класса относительно операций перестановки переменных, инвертирования переменных и инвертирования функции (геометрическая замкнутость). *Геометрическим типом функции* f назовём класс эквивалентности относительно указанных преобразований. Для булевых функций от трёх переменных доказано, что только геометрический тип с представителем $f^*(x_1, x_2, x_3) = x_1x_3 \vee x_2\overline{x_3}$ не задаётся через АПФ. Для булевых функций от четырёх

переменных существует 222 геометрических типа, из них 70 представителей содержат в качестве подфункции функцию от трёх переменных f^* и поэтому не относятся к классу АПФ. Для 101 из оставшихся 152 геометрических типов найдено задание в виде АПФ. Важно отметить, что класс АПФ замкнут относительно фиксации переменных и включает в себя все линейные функции k-значной логики.

Любое преобразование $F : \Omega_2^4 \to \Omega_2^4$, порождающее подстановку степени 16, задаётся набором координатных функций $F = (f_0, f_1, f_2, f_3)$, где $f_i : \Omega_2^4 \to \Omega_2$, $i = 0, 1, 2, 3$.

Определение 2. *АПФ-реализацией* преобразования F будем называть некоторое задание его координатных функций через булевы линейные комбинации АПФ:

$$\left(f_0^{\downarrow}, f_1^{\downarrow}, f_2^{\downarrow}, f_3^{\downarrow}\right) = \left(\varphi_0^{\downarrow}, \varphi_1^{\downarrow}, \ldots, \varphi_{n-1}^{\downarrow}\right) \begin{pmatrix} \alpha_0^0 & \alpha_0^1 & \alpha_0^2 & \alpha_0^3 \\ \alpha_1^0 & \alpha_1^1 & \alpha_1^2 & \alpha_1^3 \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{n-1}^0 & \alpha_{n-1}^1 & \alpha_{n-1}^2 & \alpha_{n-1}^3 \end{pmatrix}, \quad \varphi_i^{\downarrow} \in AT_4^2, \quad \alpha_r^m \in \Omega_2,$$

где AT_4^2 — множество всех АПФ от четырех переменных двузначной логики.

Утверждение 1. Для любого преобразования $F : \Omega_2^4 \to \Omega_2^4$ существует АПФ-реализация.

Построение АПФ-реализаций подстановок представляет собой сложную задачу дискретной математики, для решения которой может быть предложен алгоритм 1.

Алгоритм позволяет находить с высокой вероятностью АПФ-реализации подстановок, у которых в линейных комбинациях участвуют только пять АПФ.

В алгоритме используется подмножество $G(f_0, f_1, f_2, f_3)$ множества всех подфункций координатных функций f_0, f_1, f_2, f_3 подстановки π, формируемое по одному из следующих правил.

С п о с о б 1. $G(f_0, f_1, f_2, f_3) = \{f_i \wedge f_j : i \neq j\}$.

С п о с о б 2. $G(f_0, f_1, f_2, f_3) = \{g : g \wedge f_i = g, |g| = 4\}$, где $|g|$ — вес функции, $i \in \{1, \ldots, 4\}$ — фиксированное.

1. Результаты применения алгоритма 1 к подстановкам алгоритмов блочного шифрования Магма и 2-ГОСТ

Задания подстановок алгоритмов блочного шифрования Магма и 2-ГОСТ получены в [2]. Предложенные в данной работе АПФ-реализации отличаются тем, что для каждой подстановки используется система из пяти АПФ и линейные комбинации каждой координатной функции используют не более чем две из них. Задания подстановок алгоритмов блочного шифрования Магма и 2-ГОСТ можно найти в [3, 4], ниже используются обозначения из работы [2]. В табл. 1 и 2 предложены АПФ-реализации данных подстановок. В табл. 1 для каждой подстановки π_i указана функция f_4^i из множества $G(f_0, f_1, f_2, f_3)$, с использованием которой получена АПФ-реализация.

Алгоритм 1. Алгоритм нахождения АПФ-реализаций подстановок

Вход: функции f_0, f_1, f_2, f_3, множество $G(f_0, f_1, f_2, f_3)$.
Выход: АПФ-реализации $f_j = \sum\limits_i \alpha_i^j \varphi_i$, $j = 0, 1, 2, 3$, где φ_i — АПФ, либо сообщение «Не успех».

1: Из всех АПФ вида

$$\beta_0 f_0 \oplus \beta_1 f_1 \oplus \beta_2 f_2 \oplus \beta_3 f_3$$

формируем множество V, где $\beta_0, \beta_1, \beta_2, \beta_3 \in \Omega_2$.

2: Находим максимальную линейно независимую подсистему V' множества V. Если она содержит 4 функции, то переходим на шаг 3, иначе на шаг 4.

3: Пусть $V' = \{\varphi_0, \varphi_1, \varphi_2, \varphi_3\}$. Найдём решение системы

$$\left(f_0^{\downarrow}, f_1^{\downarrow}, f_2^{\downarrow}, f_3^{\downarrow}\right) = \left(\varphi_0^{\downarrow}, \varphi_1^{\downarrow}, \varphi_2^{\downarrow}, \varphi_3^{\downarrow}\right) \begin{pmatrix} \alpha_0^0 & \alpha_0^1 & \alpha_0^2 & \alpha_0^3 \\ \alpha_1^0 & \alpha_1^1 & \alpha_1^2 & \alpha_1^3 \\ \alpha_2^0 & \alpha_2^1 & \alpha_2^2 & \alpha_2^3 \\ \alpha_3^0 & \alpha_3^1 & \alpha_3^2 & \alpha_3^3 \end{pmatrix}.$$

Найденное решение подаём на выход. Конец алгоритма.

4: Если $G(f_0, f_1, f_2, f_3) = \varnothing$, то выдаём сообщение «Неуспех» и завершаем алгоритм. Иначе исключаем из множества $G(f_0, f_1, f_2, f_3)$ произвольную функцию g и переходим на шаг 5.

5: Формируем множество V, состоящее из всех АПФ вида

$$\beta_0 f_0 \oplus \beta_1 f_1 \oplus \beta_2 f_2 \oplus \beta_3 f_3 \oplus \beta_4 g.$$

6: Находим максимальную линейно независимую подсистему V' множества V. Если $V' = \{\varphi_0, \varphi_1, \varphi_2, \varphi_3, \varphi_4\}$, то на выход подаём решение системы

$$\left(f_0^{\downarrow}, f_1^{\downarrow}, f_2^{\downarrow}, f_3^{\downarrow}\right) = \left(\varphi_0^{\downarrow}, \varphi_1^{\downarrow}, \varphi_2^{\downarrow}, \varphi_3^{\downarrow}, \varphi_4^{\downarrow}\right) \begin{pmatrix} \alpha_0^0 & \alpha_0^1 & \alpha_0^2 & \alpha_0^3 \\ \alpha_1^0 & \alpha_1^1 & \alpha_1^2 & \alpha_1^3 \\ \alpha_2^0 & \alpha_2^1 & \alpha_2^2 & \alpha_2^3 \\ \alpha_3^0 & \alpha_3^1 & \alpha_3^2 & \alpha_3^3 \\ \alpha_4^0 & \alpha_4^1 & \alpha_4^2 & \alpha_4^3 \end{pmatrix}.$$

В противном случае переходим на шаг 4.

Таблица 1

АПФ-реализации подстановок алгоритма блочного шифрования Магма

π_0 : $f_4^0 = f_0^0 \wedge f_1^0$;	π_1 : $f_4^1 = f_0^1 \wedge f_1^1$;
$\varphi_0^0 : ((0,1,3,2,6);2;7)$; $f_0^0 = \varphi_0^0 \oplus \varphi_3^0$; $\varphi_1^0 : ((0,2,3,3,1);6;8)$; $f_1^0 = \varphi_1^0 \oplus \varphi_3^0$; $\varphi_2^0 : ((1,6,7,2,5);4;8)$; $f_2^0 = \varphi_0^0 \oplus \varphi_4^0$; $\varphi_3^0 : ((1,7,6,5,5);6;8)$; $f_3^0 = \varphi_2^0 \oplus \varphi_4^0$. $\varphi_4^0 : ((4,2,7,2,5);4;8)$.	$\varphi_0^1 : ((0,3,1,3,0);2;4)$; $f_0^1 = \varphi_3^1 \oplus \varphi_4^1$; $\varphi_1^1 : ((1,3,1,5,6);6;8)$; $f_1^1 = \varphi_1^1 \oplus \varphi_2^1$; $\varphi_2^1 : ((3,4,2,6,3);2;7)$; $f_2^1 = \varphi_0^1 \oplus \varphi_4^1$; $\varphi_3^1 : ((4,3,7,5,2);4;8)$; $f_3^1 = \varphi_0^1$. $\varphi_4^1 : ((5,7,5,2,5);4;8)$.
π_2 : $f_4^2 = (1100000010100000) \subset f_1^2$;	π_3 : $f_4^3 = f_1^3 \wedge f_2^3$;
$\varphi_0^2 : ((0,1,1,1,3);4;6)$; $f_0^2 = \varphi_0^2 \oplus \varphi_3^2$; $\varphi_1^2 : ((0,3,7,2,5);4;8)$; $f_1^2 = \varphi_0^2 \oplus \varphi_2^2$; $\varphi_2^2 : ((3,1,3,5,1);2;6)$; $f_2^2 = \varphi_1^2$; $\varphi_3^2 : ((3,2,1,4,3);3;6)$; $f_3^2 = \varphi_1^2 \oplus \varphi_4^2$. $\varphi_4^2 : ((4,6,3,6,7);4;8)$.	$\varphi_0^3 : ((0,2,3,1,2);2;4)$; $f_0^3 = \varphi_0^3 \oplus \varphi_1^3$; $\varphi_1^3 : ((0,5,5,5,2);3;6)$; $f_1^3 = \varphi_2^3 \oplus \varphi_3^3$; $\varphi_2^3 : ((1,3,5,4,1);6;8)$; $f_2^3 = \varphi_2^3 \oplus \varphi_4^3$; $\varphi_3^3 : ((1,6,3,2,4);5;7)$; $f_3^3 = \varphi_0^3 \oplus \varphi_4^3$. $\varphi_4^3 : ((2,4,1,2,1);2;6)$.
π_4 : $f_4^4 = f_0^4 \wedge f_1^4$;	π_5 : $f_4^5 = (0011010000000010) \subset f_1^5$;
$\varphi_0^4 : ((0,1,2,1,0);3;4)$; $f_0^4 = \varphi_2^4 \oplus \varphi_4^4$; $\varphi_1^4 : ((0,2,1,3,0);2;4)$; $f_1^4 = \varphi_0^4 \oplus \varphi_4^4$; $\varphi_2^4 : ((0,2,7,5,4);6;8)$; $f_2^4 = \varphi_3^4 \oplus \varphi_4^4$; $\varphi_3^4 : ((1,7,3,2,2);4;8)$; $f_3^4 = \varphi_1^4$. $\varphi_4^4 : ((6,1,3,3,6);6;8)$.	$\varphi_0^5 : ((5,4,1,2,6);3;8)$; $f_0^5 = \varphi_1^5 \oplus \varphi_4^5$; $\varphi_1^5 : ((0,1,6,5,4);6;8)$; $f_1^5 = \varphi_2^5 \oplus \varphi_3^5$; $\varphi_2^5 : ((0,3,0,3,2);2;4)$; $f_2^5 = \varphi_0^5 \oplus \varphi_2^5$; $\varphi_3^5 : ((0,3,4,5,1);3;6)$; $f_3^5 = \varphi_1^5 \oplus \varphi_2^5$. $\varphi_4^5 : ((5,2,5,6,7);3;8)$.
π_6 : $f_4^6 = (0001010000001001) \subset f_0^6$;	π_7 : $f_4^7 = f_0^7 \wedge f_1^7$;
$\varphi_0^6 : ((0,0,1,0,1);1;2)$; $f_0^6 = \varphi_3^6 \oplus \varphi_4^6$; $\varphi_1^6 : ((0,5,2,4,1);3;8)$; $f_1^6 = \varphi_0^6 \oplus \varphi_1^6$; $\varphi_2^6 : ((0,5,7,6,4);5;8)$; $f_2^6 = \varphi_0^6 \oplus \varphi_2^6$; $\varphi_3^6 : ((2,4,3,2,1);2;5)$; $f_3^6 = \varphi_1^6 \oplus \varphi_3^6$. $\varphi_4^6 : ((6,2,3,1,6);5;8)$.	$\varphi_0^7 : ((4,3,7,6,5);4;8)$; $f_0^7 = \varphi_0^7$; $\varphi_1^7 : ((3,3,1,5,6);2;8)$; $f_1^7 = \varphi_1^7 \oplus \varphi_4^7$; $\varphi_2^7 : ((3,3,2,5,5);3;6)$; $f_2^7 = \varphi_2^7 \oplus \varphi_3^7$; $\varphi_3^7 : ((5,2,6,3,1);4;8)$; $f_3^7 = \varphi_2^7 \oplus \varphi_4^7$. $\varphi_4^7 : ((6,3,6,5,4);6;8)$.

Таблица 2

АПФ-реализации подстановок алгоритма блочного шифрования 2-ГОСТ

π' :	π'' :
$\varphi_0' : ((0,1,5,2,2);6;9)$; $\varphi_1' : ((0,5,5,1,6);2;7)$; $f_0' = \varphi_4'$; $\varphi_2' : ((7,6,5,6,1);4;8)$; $f_1' = \varphi_2'$; $\varphi_3' : ((2,5,7,3,2);4;8)$; $f_2' = \varphi_2' \oplus \varphi_3'$; $\varphi_4' : ((3,5,1,2,3);4;8)$. $f_3' = \varphi_0' \oplus \varphi_1'$.	$\varphi_0'' : ((6,5,5,2,1);6;8)$; $\varphi_1'' : ((3,2,4,1,5);6;8)$; $f_0'' = \varphi_3'' \oplus \varphi_4''$; $\varphi_2'' : ((3,1,6,3,4);5;7)$; $f_1'' = \varphi_0'' \oplus \varphi_3''$; $\varphi_3'' : ((2,1,6,3,2);4;8)$; $f_2'' = \varphi_0'' \oplus \varphi_2''$; $\varphi_4'' : ((0,3,2,2,1);4;8)$. $f_3'' = \varphi_0'' \oplus \varphi_1''$.

ЛИТЕРАТУРА

1. *Сошин Д. А.* Представление геометрических типов булевых функций от трех переменных алгебраическими пороговыми функциями // Прикладная дискретная математика. 2016. № 1(31). С. 32–45.
2. *Сошин Д. А.* Задание подстановок алгоритмов блочного шифрования Магма и 2-ГОСТ с помощью алгебраических пороговых функций // Прикладная дискретная математика. 2016. № 3(33). С. 53–66.
3. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2015.
4. *Дмух А. А., Дыгин Д. М., Маршалко Г. Б.* Пригодная для низкоресурсной реализации модификация блочного шифра ГОСТ // Математические вопросы криптографии. 2014. Т. 5. № 2. С. 47–55.