таких n, m, для которых выполняется следующее условие:

$$m \leqslant 2^{\lceil (n+1)/2 \rceil} - 1.$$

ЛИТЕРАТУРА

1. *Meier W., Pasalic E., and Carlet C.* Algebraic attacks and decomposition of Boolean functions // Eurocrypt 2004. LNCS. 2004. V. 3027. P. 474–491.
2. *Carlet C.* On the algebraic immunities and higher order nonlinearities of vectorial Boolean functions // Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes, 2009. P. 104–116.
3. *Courtois N. and Meier W.* Algebraic attacks on stream ciphers with linear feedback // Eurocrypt 2003. LNCS. 2003. V. 2656. P. 345–359.
4. *Pokrasenko D.* On the maximal component algebraic immunity of vectorial Boolean functions // J. Appl. Industr. Math. 2016. V. 10. P. 257–263.

УДК 512.13 DOI 10.17223/2226308X/9/13

ПРЕДСТАВЛЕНИЕ ПОЛУБАЙТОВЫХ ПОДСТАНОВОК АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ МАГМА И 2-ГОСТ АЛГЕБРАИЧЕСКИМИ ПОРОГОВЫМИ ФУНКЦИЯМИ

Д. А. Сошин

Работа посвящена реализации полубайтовых подстановок алгоритмов блочного шифрования Магма и 2-ГОСТ алгебраическими пороговыми функциями (АПФ). Для каждой из подстановок алгоритмов Магма рассмотрен вопрос принадлежности линейных комбинаций координатных функций к классу АПФ. Для подстановок 2-ГОСТ предложено их задание через линейные комбинации АПФ.

Ключевые слова: *алгебраические пороговые функции, подстановки.*

В работе [1] вводится новый класс функций, который назван классом алгебраических пороговых функций.

Определение 1. Функция k-значной логики $f_n^k : \Omega_k^n \to \Omega_k$ называется *алгебраической пороговой*, если существуют целочисленные наборы $(c_0, c_1, \ldots, c_n)$, $(b_0, b_1, \ldots, b_k)$ и модуль m, такие, что для любого $\alpha \in \{0, \ldots, k-1\}$ выполняется

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

где $r_m(y)$ — *функция взятия остатка* при делении целого числа y на модуль m ($r_m(y) \in \{0, 1, \ldots, m-1\}$); $\Omega_k = \{0, 1, \ldots, k-1\}$; $\Omega_k^n = \underbrace{\Omega_k \times \Omega_k \times \cdots \times \Omega_k}_{n}$.

Тройку $((c_0, c_1, \ldots, c_n); (b_0, b_1, \ldots, b_k); m\ )$ назовём *структурой алгебраической пороговой функции* f_n^k.

В [1] проведено исследование вопроса реализации булевых функций трёх переменных функциями из класса АПФ. Для этого доказана замкнутость данного класса относительно операций перестановки переменных, инвертирования переменных в смысле Лукашевича 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 ровно 222 геометрических типа, и из них 70 представителей содержат в качестве подфункции функцию от трёх переменных, не имеющую представление в виде АПФ, и поэтому не относятся к классу АПФ. Для 99 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.

В стандарте ГОСТ Р 34.12-2015 [2] в качестве нелинейного биективного преобразования выступает набор подстановок π'_i, $i = 0, \ldots, 7$. Обозначим через $f_3^{(i)}, f_2^{(i)}, f_1^{(i)}, f_0^{(i)}$ координатные функции подстановки π'_i от старших разрядов к младшим соответственно. У каждой подстановки рассмотрены линейные комбинации координатных функций, и те, для которых нашлось АПФ-представление, приведены в табл. 1 со своими структурами.

Таблица 1

Представление линейных комбинаций координатных функций подстановок ГОСТ Р 34.12-2015 через АПФ

π'_i	Лин. комбинации	Структура АПФ	π'_i	Лин. комбинации	Структура АПФ
π'_1	$f_3^{(1)}$	$((0,3,1,3,0);(0,2,4);\ 4)$	π'_4	$f_3^{(4)}$	$((0,2,1,3,0);(0,2,4);\ 4)$
	$f_3^{(1)} \oplus f_2^{(1)} \oplus f_0^{(1)}$	$((7,5,1,3,6);(0,4,8);\ 8)$		$f_3^{(4)} \oplus f_2^{(4)} \oplus f_1^{(4)}$	$((0,5,5,6,2);(0,4,8);\ 8)$
	$f_3^{(1)} \oplus f_2^{(1)}$	$((6,1,3,6,3);(0,4,8);\ 8)$		$f_3^{(4)} \oplus f_2^{(4)} \oplus f_0^{(4)}$	$((0,6,1,6,3);(0,4,8);\ 8)$
	$f_2^{(1)} \oplus f_0^{(1)}$	$((6,3,3,1,6);(0,4,8);\ 8)$	π'_5	$f_2^{(5)} \oplus f_0^{(5)}$	$((0,3,2,5,7);(0,4,8);\ 8)$
π'_2	$f_2^{(2)}$	$((0,3,7,2,5);(0,4,8);\ 8)$		$f_2^{(5)} \oplus f_1^{(5)}$	$((6,7,5,2,6);(0,4,8);\ 8)$
	$f_1^{(2)} \oplus f_0^{(2)}$	$((1,2,5,6,3);(0,4,8);\ 8)$		$f_3^{(5)} \oplus f_2^{(5)}$	$((5,5,5,7,2);(0,4,8);\ 8)$
	$f_3^{(2)} \oplus f_2^{(2)}$	$((7,2,5,2,1);(0,4,8);\ 8)$		$f_3^{(5)} \oplus f_2^{(5)} \oplus f_0^{(5)}$	$((0,7,5,3,2);(0,4,8);\ 8)$
π'_3	$f_3^{(3)} \oplus f_0^{(3)}$	$((6,7,2,3,6);(0,4,8);\ 8)$	π'_6	$f_3^{(6)} \oplus f_1^{(6)}$	$((7,2,7,5,2);(0,4,8);\ 8)$
	$f_3^{(3)} \oplus f_2^{(3)} \oplus f_0^{(3)}$	$((3,2,7,2,5);(0,4,8);\ 8)$		$f_3^{(6)} \oplus f_2^{(6)} \oplus f_1^{(6)}$	$((6,1,6,5,6);(0,4,8);\ 8)$
π'_7	$f_0^{(7)}$	$((4,3,7,6,5);(0,4,8);\ 8)$			

Из табл. 1 видно, что функции $f_3^{(1)}$, $f_2^{(2)}$, $f_3^{(4)}$, $f_0^{(7)}$ являются алгебраическими пороговыми и имеют следующие задания:

$$f_3^{(1)} = 1 \quad \Leftrightarrow \quad r_4\left(3x_1 + 1x_2 + 3x_3\right) \geqslant 2, \quad f_2^{(2)} = 1 \quad \Leftrightarrow \quad r_8\left(3x_1 + 7x_2 + 2x_3 + 5x_4\right) \geqslant 4,$$
$$f_3^{(4)} = 1 \quad \Leftrightarrow \quad r_4\left(2x_1 + 1x_2 + 3x_3\right) \geqslant 2, \quad f_0^{(7)} = 1 \quad \Leftrightarrow \quad r_8\left(4 + 3x_1 + 7x_2 + 6x_3 + 5x_4\right) \geqslant 4.$$

Важно отметить, что функции $f_3^{(1)}$ и $f_3^{(4)}$ фиктивно зависят от переменной x_4 (x_4 — старший бит входного числа). Последнее влечёт ухудшение перемешивающих свойств нелинейного слоя.

Подстановка π'_5 представляется в виде каскадного соединения АПФ

$$\pi'_5 = \begin{pmatrix} f_3^{(5)} \\ f_2^{(5)} \\ f_1^{(5)} \\ f_0^{(5)} \end{pmatrix} = \begin{pmatrix} \varphi^{(0)} \oplus \varphi^{(3)} \\ \varphi^{(0)} \oplus \varphi^{(2)} \oplus \varphi^{(3)} \\ \varphi^{(0)} \oplus \varphi^{(1)} \oplus \varphi^{(2)} \oplus \varphi^{(3)} \\ \varphi^{(2)} \oplus \varphi^{(3)} \end{pmatrix}.$$

Функции $\varphi^{(0)}, \varphi^{(1)}, \varphi^{(2)}, \varphi^{(3)}$ задают соответствующие линейные комбинации $f_2^{(5)} \oplus$ $\oplus f_0^{(5)}$, $f_2^{(5)} \oplus f_1^{(5)}$, $f_3^{(5)} \oplus f_2^{(5)}$, $f_3^{(5)} \oplus f_2^{(5)} \oplus f_0^{(5)}$ из табл. 1 следующим образом:

$$\varphi^{(0)} = 1 \Leftrightarrow r_8(3x_1 + 2x_2 + 5x_3 + 7x_4) \geqslant 4, \quad \varphi^{(1)} = 1 \Leftrightarrow r_8(6 + 7x_1 + 5x_2 + 2x_3 + 6x_4) \geqslant 4,$$
$$\varphi^{(2)} = 1 \Leftrightarrow r_8(5 + 5x_1 + 5x_2 + 7x_3 + 2x_4) \geqslant 4, \quad \varphi^{(3)} = 1 \Leftrightarrow r_8(7x_1 + 5x_2 + 3x_3 + 2x_4) \geqslant 4.$$

В [3] предложен алгоритм блочного шифрования 2-ГОСТ, являющийся модификацией шифрсистемы ГОСТ 28147-89, отличающийся от последней лишь алгоритмом развертывания ключа, а также тем, что набор S-боксов фиксирован: $\pi_0 = \pi_1 = \pi_2 = \pi_3 = \pi'$, $\pi_4 = \pi_5 = \pi_6 = \pi_7 = \pi''$, где π' и π'' заданы нижними строками подстановок (табл. 2).

Таблица 2

Задание подстановок 2-ГОСТ

i	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi'(i)$	6	A	F	4	3	8	5	0	D	E	7	1	2	B	C	9
$\pi''(i)$	E	0	8	1	7	A	5	6	D	2	4	9	3	F	C	B

В результате анализа подстановок π' и π'' каждую из них удалось задать через линейные комбинации пяти АПФ

$$\pi' = \begin{pmatrix} f'_3 \\ f'_2 \\ f'_1 \\ f'_0 \end{pmatrix} = \begin{pmatrix} g_1 \oplus g_2 \\ g_3 \oplus g_4 \\ g_3 \\ g_5 \end{pmatrix}, \qquad \pi'' = \begin{pmatrix} f''_3 \\ f''_2 \\ f''_1 \\ f''_0 \end{pmatrix} = \begin{pmatrix} v_1 \oplus v_2 \\ v_1 \oplus v_3 \\ v_1 \oplus v_4 \\ v_4 \oplus v_5 \end{pmatrix},$$

где функции $g_1, g_2, g_3, g_4, g_5, v_1, v_2, v_3, v_4, v_5$ — алгебраические пороговые:

$$\begin{aligned}
g_1 &= 1 \Leftrightarrow r_9\,(x_1 + 5x_2 + 2x_3 + 2x_4) \geqslant 6, & v_1 &= 1 \Leftrightarrow r_8\,(6 + 5x_1 + 5x_2 + 2x_3 + x_4) \geqslant 6,\\
g_2 &= 1 \Leftrightarrow r_7\,(5x_1 + 5x_2 + x_3 + 6x_4) \geqslant 2, & v_2 &= 1 \Leftrightarrow r_8\,(3 + 2x_1 + 4x_2 + x_3 + 5x_4) \geqslant 6,\\
g_3 &= 1 \Leftrightarrow r_8\,(7 + 6x_1 + 5x_2 + 6x_3 + x_4) \geqslant 4, & v_3 &= 1 \Leftrightarrow r_7\,(3 + x_1 + 6x_2 + 3x_3 + 4x_4) \geqslant 5,\\
g_4 &= 1 \Leftrightarrow r_8\,(2 + 5x_1 + 7x_2 + 3x_3 + 2x_4) \geqslant 4, & v_4 &= 1 \Leftrightarrow r_8\,(2 + x_1 + 6x_2 + 3x_3 + 2x_4) \geqslant 4,\\
g_5 &= 1 \Leftrightarrow r_8\,(3 + 5x_1 + x_2 + 2x_3 + 3x_4) \geqslant 4, & v_5 &= 1 \Leftrightarrow r_8\,(3x_1 + 2x_2 + 2x_3 + x_4) \geqslant 4.
\end{aligned}$$

Здесь x_1 — младший бит входного числа, x_4 — старший.

Класс АПФ сохраняет простоту реализации функций, основная сложность которой сводится к подсчёту скалярного произведения, как и для пороговых функций.

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. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2015.
3. *Дмух А. А., Дыгин Д. М., Маршалко Г. Б.* Пригодная для низкоресурсной реализации модификация блочного шифра ГОСТ // Матем. вопр. криптограф. 2014. Т. 5. № 2. С. 47–55.