УДК 519.7

М.А. ПУДОВКИНА

Национальный исследовательский ядерный университет «МИФИ», Москва

ОРТОМОРФНЫЕ ПРЕОБРАЗОВАНИЯ РЕГИСТРОВ СДВИГА НАД ПОЛЕМ $GF(2^m)$

В настоящее время ортоморфизмы используются при синтезе алгоритмов поточного и блочного шифрования. Проблема их построения в общем случае является открытой. В работе получены достаточные условия ортоморфности класса нелинейных преобразований регистров сдвига. Приведены примеры таких преобразований. Получен критерий ортоморфности композиции линейных регистровых преобразований. Показано, что критерию удовлетворяет MDS-матрица алгоритма «Кузнечик».

Преобразования регистров сдвига над конечными полями традиционно используются при синтезе блочных и поточных шифрсистем. В данной работе рассматривается класс биективных регистровых преобразований $\rho_v^{(n)}$ на n-мерном векторном пространстве $V_n(2^m)$ над полем $GF(2^m)$ с функцией обратной связи $v: V_n(2^m) \to GF(2^m)$, заданных условиями

$$\rho_v^{(n)} : (x_1, ..., x_n) \mapsto (x_2, ..., x_n, v(x_1, ..., x_n)) \quad (1)$$

и являющихся ортоморфизмами, т.е. отображение

$$\tilde{\rho}_v^{(n)} : (x_1, ..., x_n) \mapsto (x_2 - x_1, ..., x_n - x_{n-1}, v(x_1, ..., x_n) - x_n)$$

есть подстановка на $V_n(2^m)$. Несложно убедиться, что если отображение v линейно,

$$v(x_1, ..., x_n) = \sum_{i=1}^{n} c_i x_i, \quad c_1, ..., c_n \in GF(2^m),$$

то для ортоморфности достаточно проверить условие $c_1 \neq 0$, $\sum_{i=1}^{n} c_i \neq 1$. Однако, для нелинейных преобразований проблема построения ортоморфизмов остается открытой (например, [1, 2]). В данной работе получено достаточное условие ортоморфности преобразования $\rho_v^{(n)}$.

Утверждение 1. *Пусть* $m, n \in \mathbb{N}$, $m \geq 1$, $n \geq 3$, *преобразования* $v: V_n(2^m) \to GF(2^m)$ *задано условием:*

$$v(x_1, ..., x_n) = c_1 x_1^{d_1} + c_2 x_2^{d_2} + ... + c_n x_n^{d_n},$$

где набор $(c_1,...,c_n) \in V_n(2^m)$ *и числа* $d_1,...,d_n \in \{1,...,2^m-2\}$, $p \in \{1,...,n\}$ *таковы, что:*

$$c_j \neq 0,\ \text{НОД}(d_j, 2^m-1) = 1 \text{ для каждого } j \in \{1,p\},$$

$$\{d_i \mid i \in \{1,...,n\} \setminus \{p\}, c_i \neq 0\} \subseteq \{2^t \mid t \in \{0,...,m-1\}\},$$

а преобразование $\tilde{v} : GF(2^m) \to GF(2^m)$,

$$\tilde{v} : y \mapsto v(y,...,y,y) + y \text{ для каждого } y \in GF(2^m),$$

есть подстановка на $GF(2^m)$. *Тогда* $\rho_v^{(n)}$ *есть ортоморфизм.*

Отметим, что при $m=1$ утверждению 1 удовлетворяют только линейные функции обратной связи, у которых число существенных переменных четно, а x_1 существенна. При $m>1$ приведены примеры функций обратной связи v, при которых $\rho_v^{(n)}$ – ортоморфизм. Выясним, для каких линейных функций обратной связи v и степеней $r \in \mathbb{N}$ преобразование $(\rho_v^{(n)})^r$ есть ортоморфизм.

Утверждение 2. *Пусть* $m, r \in \mathbb{N}$, $n \geq 3$, $v : V_n(2^m) \to GF(2^m)$, $\rho_v^{(n)} : V_n(2^m) \to V_n(2^m)$ *заданы условиями:*

$$v(x_1,...,x_n) = c_1x_1 + c_2x_2 + ... + c_nx_n,$$

где $(c_1,c_2,...,c_n) \in V_n(2^m)$, $c_1 \neq 0$. *Пусть также орграф* $\Gamma(\rho_v^{(n)}) = \left(V_n(2^m), \Lambda_v^{(n)}\right)$ *линейного преобразования* $\rho_v^{(n)}$ *на множестве* $V_n(2^m) \setminus \{0_n\}$ *имеет* s *циклов длин* $l_1,...,l_s$. *Тогда и только тогда* $(\rho_v^{(n)})^r$ *есть ортоморфизм, когда* $r \not\equiv 0 \pmod{l_d}$ *для каждого* $d \in \{1,...,s\}$.

Показано, что утверждению 2 удовлетворяет MDS-матрица линейного слоя алгоритма блочного шифрования «Кузнечик» [3].

Список литературы

1. Johnson D.M., Dulmage A.L., Mendelsohn N.S. Orthomorphisms of groups and orthogonal Latin squares, I. Canad. J. Math. 1961, v.13, p. 356–372.

2. Denes J., Keedwell A.D. Latin squares and their applications. London: English Univ. Press, 1975.

3. Погорелов Б. А., Пудовкина М. А. Обобщенные квази-адамаровы преобразования на конечных группах. Математические вопросы криптографии. т. 13, № 4, с. 97–124, 2022.

4. Информационная технология (ИТ). Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2016.