8. *Junod P. and Vaudenay S.* FOX: A new family of block ciphers // Selected Areas in Cryptography'04. LNCS. 2005. V. 3357. P. 114–129.
9. *Gilboa S. and Gueron S.* Balanced permutations Even-Mansour ciphers // Cryptology ePrint Archive. 2014. Report 2014/642.
10. *Massey J. L.* SAFER K-64: a byte-oriented block-ciphering algorithm // FSE'94. LNCS. 1994. V. 809. P. 1–17.

УДК 519.7 DOI 10.17223/2226308X/12/7

О КЛАССЕ СТЕПЕННЫХ КУСОЧНО-АФФИННЫХ ПОДСТАНОВОК НА НЕАБЕЛЕВОЙ ГРУППЕ ПОРЯДКА 2^m, ОБЛАДАЮЩЕЙ ЦИКЛИЧЕСКОЙ ПОДГРУППОЙ ИНДЕКСА ДВА

Б. А. Погорелов, М. А. Пудовкина

Четыре неабелевы группы порядка 2^m, $m \geqslant 4$, имеют циклические подгруппы индекса два. Примерами являются широко известная группа диэдра и обобщённая группа кватернионов. Произвольная неабелева группа G порядка 2^m, обладающая циклической подгруппой индекса два, в определённом смысле близка к встречающейся в качестве группы наложения ключа аддитивной абелевой группе кольца вычетов $\mathbb{Z}_{2^m}$. В данной работе на группе G задаются два класса преобразований, названных степенными кусочно-аффинными, для которых доказаны критерии биективности. Они позволят далее провести полную классификацию ортоморфизмов, полных преобразований и их вариаций во множестве всех степенных кусочно-аффинных подстановок.

Ключевые слова: *неабелева группа, группа диэдра, обобщённая группа кватернионов, критерий биективности, ортоморфизм.*

В ARX-шифрсистемах используются просто реализуемые операции сложения в кольце вычетов, в векторном пространстве над полем GF(2), а также циклический сдвиг. Возникает вопрос о переходе к просто реализуемой группе наложения ключа, относительно которой вместе с некоторым преобразованием g могут эффективно обеспечиваться перемешивающие и рассеивающие свойства.

Неабелевы группы порядка 2^m, обладающие циклической подгруппой индекса два, в определенном смысле преемственны широко встречающимся в качестве групп наложения ключа аддитивным абелевым группами m-мерного векторного пространства $V_m(2)$ над полем GF(2) и кольца вычетов $\mathbb{Z}_{2^m}$. В [1] описана связь между неабелевостью группы наложения ключа и свойством марковости алгоритмов блочного шифрования.

Из теоремы 12.5.1 [2] следует, что неабелевыми группами порядка 2^m, имеющими циклическую подгруппу индекса два, являются только четыре группы с двумя образующим a, u, удовлетворяющими следующим определяющим соотношениям:

1) обобщённая группа кватернионов Q_{2^m}, $m \geqslant 3$,

$$a^{2^{m-1}} = e,\ u^2 = a^{2^{m-2}},\ ua = a^{-1}u;$$

2) группа диэдра $D_{2^{m-1}}$, $m \geqslant 3$,

$$a^{2^{m-1}} = e,\ u^2 = e,\ ua = a^{-1}u;$$

3) $m \geqslant 4$,

$$a^{2^{m-1}} = e,\ u^2 = e,\ ua = a^{1+2^{m-2}}u;$$

4) $m \geqslant 4$,

$$a^{2^{m-1}} = e,\ u^2 = e,\ ua = a^{-1+2^{m-2}}u.$$

На произвольной неабелевой группе $G = \langle a, u\rangle$ порядка 2^m, имеющей циклическую подгруппу $\langle a\rangle$ индекса два, рассмотрим преобразования двух видов $\theta^{(r_1,r_2,q_1,q_2)}_{(c_1,c_2,b_1,b_2)} : G \to G$ и $\tilde{\theta}^{(r_1,r_2,q_1,q_2)}_{(c_1,c_2,b_1,b_2)} : G \to G$, заданные условиями

$$\theta^{(r_1,r_2,q_1,q_2)}_{(c_1,c_2,b_1,b_2)} : a^i \mapsto \begin{cases} a^{r_1 i+c_1}, & \text{если } i \in \{0,\dots,2^{m-2}-1\},\\ a^{r_2 i+c_2}u, & \text{если } i \in \{2^{m-2},\dots,2^{m-1}-1\},\end{cases}$$

$$\theta^{(r_1,r_2,q_1,q_2)}_{(c_1,c_2,b_1,b_2)} : a^i u \mapsto \begin{cases} a^{q_1 i+b_1}u, & \text{если } i \in \{0,\dots,2^{m-2}-1\},\\ a^{q_2 i+b_2}, & \text{если } i \in \{2^{m-2},\dots,2^{m-1}-1\},\end{cases}$$

$$\tilde{\theta}^{(r_1,r_2,q_1,q_2)}_{(c_1,c_2,b_1,b_2)} : a^i \mapsto \begin{cases} a^{r_1 i+c_1}, & \text{если } i \in \{0,\dots,2^{m-2}-1\},\\ a^{r_2 i+c_2}u, & \text{если } i \in \{2^{m-2},\dots,2^{m-1}-1\},\end{cases}$$

$$\tilde{\theta}^{(r_1,r_2,q_1,q_2)}_{(c_1,c_2,b_1,b_2)} : a^i u \mapsto \begin{cases} a^{q_1 i+b_1}, & \text{если } i \in \{0,\dots,2^{m-2}-1\},\\ a^{q_2 i+b_2}u, & \text{если } i \in \{2^{m-2},\dots,2^{m-1}-1\},\end{cases}$$

где $b_1, b_2, c_1, c_2 \in \{0,\dots,2^{m-1}-1\}$, $r_1, r_2, q_1, q_2 \in \{0,\dots,2^{m-1}-1\}$.

Далее преобразования $\theta^{(r_1,r_2,q_1,q_2)}_{(c_1,c_2,b_1,b_2)}$ и $\tilde{\theta}^{(r_1,r_2,q_1,q_2)}_{(c_1,c_2,b_1,b_2)}$ будем называть *степенными кусочно-аффинными*. Для каждого из этих преобразований получены критерии биективности. Приведём критерий для преобразования $\theta^{(r_1,r_2,q_1,q_2)}_{(c_1,c_2,b_1,b_2)}$.

Теорема 1. Пусть $m \geqslant 4$, $G = \langle a, u\rangle$, G — неабелева группа порядка 2^m с циклической подгруппой $\langle a\rangle$ индекса два. Преобразование $\theta^{(r_1,r_2,q_1,q_2)}_{(c_1,c_2,b_1,b_2)} : G \to G$ является подстановкой тогда и только тогда, когда элементы $b_1, b_2, c_1, c_2 \in \{0,\dots,2^{m-1}-1\}$, $r_1, r_2, q_1, q_2 \in \{0,\dots,2^{m-1}-1\}$ удовлетворяют одному из следующих условий:

1. Если $r_1 \equiv r_2 \equiv 1 \pmod 2$, то
   - 1.1. $r_1 = q_2$, $r_2 = q_1$, $c_1 = b_2$, $c_2 = b_1$;
   - 1.2. $r_1 = q_2$, $r_2 = 2^{m-1} - q_1$, $c_1 = b_2$, $b_1 - c_2 + 2^{m-2} \equiv q_1 \pmod{2^{m-1}}$;
   - 1.3. $r_2 = q_1$, $r_1 = 2^{m-1} - q_2$, $c_2 = b_1$, $b_2 - c_1 + 2^{m-2} \equiv q_2 \pmod{2^{m-1}}$;
   - 1.4. $r_2 = 2^{m-1} - q_1$, $r_1 = 2^{m-1} - q_2$, $b_1 - c_2 + 2^{m-2} \equiv q_1 \pmod{2^{m-1}}$, $b_2 - c_1 + 2^{m-2} \equiv q_2 \pmod{2^{m-1}}$.
2. Если $r_1 \equiv 1 \pmod 2$, $r_2 \equiv q_1 \equiv 2 \pmod 4$, то
   - 2.1. $r_1 = q_2$, $c_1 = b_2$, $b_1 + c_2 \equiv 1 \pmod 2$;
   - 2.2. $r_1 = 2^{m-1} - q_2$, $b_1 + c_2 \equiv 1 \pmod 2$, $b_2 - c_1 + 2^{m-2} \equiv q_2 \pmod{2^{m-1}}$.
3. Если $r_2 \equiv 1 \pmod 2$, $r_1 \equiv q_2 \equiv 2 \pmod 4$, то
   - 3.1. $r_2 = q_1$, $c_2 = b_1$, $b_2 + c_1 \equiv 1 \pmod 2$;
   - 3.2. $r_2 = 2^{m-1} - q_1$, $c_1 = b_2$, $b_1 + c_2 \equiv 1 \pmod 2$.
4. Если $r_1 \equiv r_2 \equiv 2 \pmod 4$, то
   - 4.1. $q_1 \equiv q_2 \equiv 2 \pmod 4$, $b_1 + c_2 \equiv 1 \pmod 2$, $b_2 + c_1 \equiv 1 \pmod 2$.

Полученные критерии биективности в дальнейшем позволят для каждой из четырёх неабелевых групп порядка 2^m, обладающих циклической подгруппой индекса два, классифицировать ортоморфизмы, полные преобразования, а также левые ортоморизмы и полные левые преобразования [3] в множестве всех степенных кусочно-аффинных подстановок $\theta^{(r_1,r_2,q_1,q_2)}_{(c_1,c_2,b_1,b_2)}$, $\tilde{\theta}^{(r_1,r_2,q_1,q_2)}_{(c_1,c_2,b_1,b_2)}$.

ЛИТЕРАТУРА

1. *Погорелов Б. А., Пудовкина М. А.* О неабелевых группах наложения ключа и марковости алгоритмов блочного шифрования // Прикладная дискретная математика. Приложение. 2018. № 11. С. 79–81.
2. *Холл М.* Теория групп. М.: ИЛ, 1962. 468 с.
3. *Погорелов Б. А., Пудовкина М. А.* Вариации ортоморфизмов и псевдоадамаровых преобразований на неабелевой группе // Прикладная дискретная математика. Приложение. 2019. № 12. С. 24–27.

УДК 519.1 DOI 10.17223/2226308X/12/8

ТОЧНАЯ ФОРМУЛА ЭКСПОНЕНТА ПЕРЕМЕШИВАЮЩЕГО ОРГРАФА РЕГИСТРОВОГО ПРЕОБРАЗОВАНИЯ

В. М. Фомичев, Я. Э. Авезова

Для примитивного перемешивающего n-вершинного орграфа $\Gamma(g)$ преобразования g двоичного регистра сдвига длины n, где обратная связь $f(x_0, \ldots, x_{n-1})$ имеет m существенных переменных с множеством номеров $D(g) = \{d_1, \ldots, d_m\}$, $n \geqslant 3$, $2 \leqslant m \leqslant n$, $0 = d_1 < \ldots < d_m$, при $d_m \in \{n-1, n-2\}$ получена точная формула экспонента $\exp \Gamma(g)$ и элементарных локальных экспонентов $\gamma_{u,v}$, $0 \leqslant u, v < n$.

Ключевые слова: *локально примитивный орграф, перемешивающий орграф, примитивный орграф, регистр сдвига, экспонент орграфа.*

Введение

Изучение экспонентов примитивных матриц и графов началось в 1912 г. с работы Фробениуса [1]. Основные понятия и научные достижения отражены в обзоре [2] и ряде других работ. Получение точной аналитической формулы экспонента для того или иного класса матриц и орграфов — сложная комбинаторная задача, в связи с чем большинство работ в этой области посвящены верхним оценкам экспонентов, важным для приложений.

Исследован класс преобразований g пространства n-мерных векторов, реализуемых регистром левого сдвига с нелинейной обратной связью $f(x_0, \ldots, x_{n-1})$, имеющей m существенных переменных, в том числе x_0 (иначе реальная длина регистра меньше n), $n \geqslant 3$, $2 \leqslant m \leqslant n$. Анализ перемешивающих свойств преобразований данного класса имеет прикладное значение для ряда систем защиты информации.

Пусть множество вершин перемешивающего орграфа $\Gamma(g)$, соответствующих номерам входных переменных преобразования g, есть $\{0, \ldots, n-1\}$. Получены точные формулы экспонентов и локальных экспонентов двух частных классов перемешивающих орграфов регистровых преобразований. Первый класс орграфов имеет петлю в вершине $n-1$, второй класс содержит контур $(n-1, n-2)$ длины 2.

1. Структурные свойства перемешивающих орграфов регистровых преобразований

Рассмотрим преобразование g двоичного регистра левого сдвига длины n с нелинейной функцией обратной связи $f(x_0, \ldots, x_{n-1})$. Обозначим $D(g) = \{d_1, \ldots, d_m\}$ множество номеров всех существенных переменных функции f, где $0 = d_1 < \ldots < d_m \leqslant n-1$. Тогда преобразованию g соответствует n-вершинный перемешивающий орграф $\Gamma(g)$, имеющий $n+m-1$ дуг, где n дуг составляют гамильтонов контур $(n-1, \ldots, 0)$ и остальные дуги суть $(d_2, n-1), \ldots, (d_m, n-1)$. Таким образом, связный орграф $\Gamma(g)$ есть объ-