3. *Кузьмин А. С.* О периодах разрядов в r-ичной системе счисления знаков линейных рекуррентных последовательностей над конечными простыми полями // Безопасность информационных технологий. 1995. Вып. 4. С. 71–75.
4. *Кузьмин С. А.* Периоды разрядных последовательностей линейных рекуррент максимального периода над конечными простыми полями // Прикладная дискретная математика. 2015. № 1(27). С. 62–68.
5. *Кузьмин С. А.* О двоичных разрядных последовательностях над кольцами Галуа, допускающих эффект сокращения периода // Фундамент. и прикл. матем. 2015. Т. 20. № 1. С. 223–230.

УДК 519.7 DOI 10.17223/2226308X/9/5

О ГРУППАХ, ПОРОЖДЁННЫХ ПРЕОБРАЗОВАНИЯМИ СМЕШАННОГО ТИПА И ГРУППАМИ НАЛОЖЕНИЯ КЛЮЧА

Б. А. Погорелов, М. А. Пудовкина

Наиболее распространёнными группами наложения ключа итерационных алгоритмов блочного шифрования являются регулярное подстановочное представление V_n^+ группы векторного наложения ключа, регулярное подстановочное представление $\mathbb{Z}_{2^n}^+$ аддитивной группы кольца вычетов и регулярное подстановочное представление $\mathbb{Z}_{2^n+1}^\odot$ мультипликативной группы простого поля (2^n+1 — простое число). Рассматривается расширение группы $G_n = \langle V_n^+, \mathbb{Z}_{2^n}^+ \rangle$ преобразованиями и группами, естественными для криптографической практики. К числу таких преобразований и групп относятся: группы $\mathbb{Z}_{2^d}^+ \times V_{n-d}^+$ и $V_{n-d}^+ \times \mathbb{Z}_{2^d}^+$, подстановка псевдообращения над полем $\mathrm{GF}(2^n)$ или кольцом Галуа $\mathrm{GR}(2^{md}, 2^m)$.

Ключевые слова: *группа наложения ключа, аддитивная регулярная группа, сплетение групп подстановок, мультипликативная группа кольца вычетов, кольцо Галуа.*

Группы наложения ключа итерационных алгоритмов блочного шифрования являются, как правило, регулярными абелевыми. Среди них наиболее распространены следующие:

— V_n^+ — регулярное подстановочное представление группы векторного наложения ключа над полем $\mathrm{GF}(2)$. Оно является элементарной абелевой 2-группой и используется в AES, Р34.12-2015 «Кузнечик» и многих других алгоритмах блочного шифрования. Группа V_n^+ имеет $(2^n-1)\dots(2^n-2^{r-1})/(2^r-1)\dots(2^2-1)(2-1)$ изоморфных подгрупп порядка 2^r, $r=1,\dots,n$, и столько же систем импримитивности;

— $\mathbb{Z}_{2^n}^+$ — регулярное подстановочное представление аддитивной группы кольца вычетов. Оно используется, например, в алгоритме блочного шифрования ГОСТ 28147-89. Из цикличности группы следует, что у неё имеется $n-1$ собственных подгрупп и столько же систем импримитивности;

— $\mathbb{Z}_{2^n+1}^\odot$ — регулярное подстановочное представление мультипликативной группы простого поля, в которой элемент 2^n переобозначается как 0 (модульное умножение), а 2^n+1 — простое число. Как мультипликативная группа конечного поля она циклическая порядка 2^n с $n-1$ собственной подгруппой.

В этом смысле последние два способа наложения ключа предпочтительней, так как необходимо, чтобы слой s-боксов и линейный слой рассеивали меньшее число систем импримитивности.

Пусть $G_n = \left\langle V_n^+, \mathbb{Z}_{2^n}^+ \right\rangle$, $S(X)$ — симметрическая группа на множестве X, $G_1 \wr G_2$ — сплетение групп подстановок G_1, G_2.

В [1, 2] описано строение группы G_n и её свойства. В данной работе рассматривается расширение группа G_n преобразованиями и группами, естественными для криптографической практики. К числу таких преобразований и групп относятся: группы $\mathbb{Z}_{2^d}^+ \times V_{n-d}^+$ и $V_{n-d}^+ \times \mathbb{Z}_{2^d}^+$, подстановка псевдообращения над полем $\mathrm{GF}(2^n)$ или кольцом Галуа $\mathrm{GR}(2^{md}, 2^m)$.

Первоначально описаны свойства групп, порождённых G_n, $\mathbb{Z}_{2^d}^+ \times V_{n-d}^+$, $V_{n-d}^+ \times \mathbb{Z}_{2^d}^+$ для $d \in \{1, \ldots, n-1\}$, $n \geqslant 2$. Доказано, что если $n \geqslant 2$, то $\left\langle \mathbb{Z}_{2^d}^+ \times V_{n-d}^+, G_n \right\rangle = G_n$ для $d = 1, \ldots, n-1$ и

$$\left\langle G_n, V_{n-d}^+ \times \mathbb{Z}_{2^d}^+ \right\rangle = \begin{cases} S(V_n), & \text{если } d \in \{2, \ldots, n-1\}, \\ G_n, & \text{если } d = 1. \end{cases}$$

Кроме того,

$$\left\langle V_{d_1}^+ \times Z_{2^{d_0}}^+ \times V_{n-d}^+, G_n \right\rangle \approx S(V_d) \wr G_{n-d}$$

для любых $d \in \{3, \ldots, n\}$, $d_0 \in \{2, \ldots, n-d-1\}$, где $d_1 = n - d_0$.

Для $n \geqslant 2$ и подстановки $g_n : \mathrm{GF}(2^n) \to \mathrm{GF}(2^n)$, заданной условием

$$g_n : \lambda \mapsto \begin{cases} \lambda^{-1}, & \text{если } \lambda \neq 0, \\ 0, & \text{если } \lambda = 0, \end{cases}$$

доказаны равенства $\left\langle g_n, \mathbb{Z}_{2^n}^+ \right\rangle = \langle g_n, G_n \rangle = S(V_n)$.

Пусть $LT_2\left(\mathbb{Z}_{2^{n/2}}\right)$ — группа нижнетреугольных матриц из $GL_2\left(\mathbb{Z}_{2^{n/2}}\right)$. Для чётного числа $n \geqslant 4$ доказано, что

$$LT_2\left(\mathbb{Z}_{2^{n/2}}\right) < G_n, \langle G_n, GL_2\left(\mathbb{Z}_{2^{n/2}}\right)\rangle = S(V_n).$$

Рассмотрим теперь связь подстановочного представления $\mathbb{Z}_{2^n+1}^{\odot}$ мультипликативной группы кольца $\mathbb{Z}_{2^n+1}$ и группы G_n. Пусть $\mathbb{Z}_{2^n+1}^*$ — мультипликативная группа кольца $\mathbb{Z}_{2^n+1}$ и для произвольного числа $r \in \mathbb{Z}_{2^n+1}^*$ преобразование $b^{(r)} \in S\left(\mathbb{Z}_{2^n}\right)$ задано условием $b^{(r)} : x \mapsto rx \bmod (2^n + 1)$. Положим $B_n = \left\langle b^{(r)} : r \in \mathbb{Z}_{2^n+1}^* \right\rangle$. Доказано, что если $n \geqslant 2$, то $\langle B_n, G_n \rangle = S(V_n)$. Кроме того,

$$\langle B_d \times B_{n-d}, G_n \rangle \approx S(V_d) \wr S(V_{n-d}), \quad d = 1, \ldots, n-1.$$

Для фиксированных произвольных чисел $m, d \in \mathbb{N}$ положим $n = md$. Рассмотрим кольцо Галуа $\mathrm{GR}(2^{md}, 2^m)$. Известно [3], что существует элемент b порядка $2^d - 1$, принадлежащий мультипликативной группе кольца Галуа $\mathrm{GR}\left(2^{md}, 2^m\right)$. Рассмотрим преобразование $\tilde{u}_b^{(n)} : \mathrm{GR}\left(2^{md}, 2^m\right) \to \mathrm{GR}\left(2^{md}, 2^m\right)$, заданное условием $\tilde{u}_b^{(n)} : \alpha \mapsto b\alpha$ для каждого $\alpha \in \mathrm{GR}\left(2^{md}, 2^m\right)$. Доказаны равенства

$$\left\langle G_n, \tilde{u}_b^{(n)} \right\rangle = \left\langle G_n, GL_1\left(\mathrm{GR}(2^{md}, 2^m)\right)\right\rangle = S(V_n).$$

Положим $m = 2$, $n = 2d$ и рассмотрим кольцо Галуа $\mathrm{GR}(4^d,\ 4)$ характеристики 4. Определим биекцию $\tilde{s}_d^{(2)} : \mathrm{GR}(4^d,\ 4) \to \mathrm{GR}(4^d,\ 4)$ условием

$$\tilde{s}_d^{(2)} : 2\alpha_1 + \alpha_0 \mapsto \begin{cases} \alpha\alpha_0^{-2}, & \text{если } \alpha_0 \neq 0, \\ 2\alpha_1^{-1}, & \text{если } \alpha_0 = 0, \alpha_1 \neq 0, \\ 0, & \text{если } \alpha_0 = \alpha_1 = 0, \end{cases}$$

для каждого элемента $\alpha = 2\alpha_1 + \alpha_0 \in \mathrm{GR}(4^d, 4)$, где $\alpha_0, \alpha_1 \in \mathrm{GF}(2^d)$. Преобразование $\tilde{s}_d^{(2)}$ является аналогом подстановки g_n. Очевидно, что $\tilde{s}_d^{(2)}$ — инволюция. Доказано, что $\left\langle \tilde{s}_d^{(2)}, G_n \right\rangle = S(V_d) \wr S(V_d)$.

ЛИТЕРАТУРА

1. *Погорелов Б. А., Пудовкина М. А.* Надгруппы аддитивных регулярных групп порядка 2^n кольца вычетов и векторного пространства // Дискретная математика. 2015. Т. 27. № 3. С. 74–94.
2. *Погорелов Б. А., Пудовкина М. А.* Орбитальные производные по подгруппам и их комбинаторно-групповые свойства // Дискретная математика. 2015. Т. 27. № 4. С. 94–119.
3. *Елизаров В. П.* Конечные кольца. М.: Гелиос АРВ, 2006.

УДК 519.7 DOI 10.17223/2226308X/9/6

О КЛАССИФИКАЦИИ ДИСТАНЦИОННО-ТРАНЗИТИВНЫХ ГРАФОВ ОРБИТАЛОВ НАДГРУПП ГРУППЫ ДЖЕВОНСА

Б. А. Погорелов, М. А. Пудовкина

Группа экспоненцирования $S_2 \uparrow S_n$, называемая также группой Джевонса, совпадает с группой $A\tilde{S}_n$, порождённой группой сдвигов на n-мерном векторном пространстве V_n над полем $\mathrm{GF}(2)$ и группой подстановочных $(n \times n)$-матриц $\tilde{S}_n$ над полем $\mathrm{GF}(2)$. Для группы подстановок $G \geqslant S_2 \uparrow S_n$ рассматривается её естественное действие на упорядоченных парах векторов из пространства V_n. Орбиты при таком действии называются орбиталами. Каждому орбиталу Γ ставится в соответствие граф с множеством вершин V_n и множеством рёбер Γ, называемый графом орбитала. Проводится классификация дистанционно-транзитивных графов орбиталов надгрупп группы Джевонса. Показано, что среди дистанционно-транзитивных графов орбиталов надгрупп группы Джевонса имеются графы, изоморфные следующим графам: полному графу K_{2^n}, полному двудольному графу $K_{2^{n-1},2^{n-1}}$, половинному $(n+1)$-кубу, сложенному $(n+1)$-кубу, графам знакопеременных форм, графу Тейлора, графу Адамара.

Ключевые слова: *граф орбитала, группа Джевонса, дистанционно-транзитивный граф, граф Хемминга.*

Группа экспоненцирования $S_2 \uparrow S_n$, называемая также группой Джевонса, совпадает с группой $A\tilde{S}_n$, порождённой группой сдвигов на n-мерном векторном пространстве V_n над полем $\mathrm{GF}(2)$ и группой подстановочных $(n \times n)$-матриц $\tilde{S}_n$ над полем $\mathrm{GF}(2)$. Группа Джевонса встречается в теории кодирования, теории графов, теории булевых функций, алгебраической комбинаторике и криптографии; в частности, она

— является группой изометрий метрики Хемминга на V_n;
— описывает множество преобразований, не распространяющих искажения;
— является группой инерции множества всех бент-функций.

Для группы подстановок $G \geqslant S_2 \uparrow S_n$ рассматривается также её естественное действие на упорядоченных парах векторов из пространства V_n. Орбиты при таком действии называются орбиталами. Каждому орбиталу Γ ставится в соответствие граф $\bar{\Gamma} = (V_n, \Gamma)$ с множеством вершин V_n и множеством рёбер Γ, называемый графом орбитала. В алгебраической комбинаторике группа Джевонса связана со схемой отношений Хемминга [1] на пространстве V_n, которая может задаваться алгеброй матриц смежности графов орбиталов группы $A\tilde{S}_n$. При этом орбиталы пронумерова-