ЛИТЕРАТУРА

1. *Tokareva N. N.* Bent functions: results and applications to cryptography. Acad. Press. Elsevier, 2015. 230 p.
2. *Tokareva N. N.* Duality between bent functions and affine functions // Discr. Math. 2012. V. 312. Iss. 3. P. 666–670.
3. *Solé P.* Completely regular codes and completely transitive codes // Discr. Math. 1990. V. 81. Iss. 2. P. 193–201.
4. *Delsarte P.* An Algebraic Approach to the Association Schemes of Coding Theory. Thesis. Universite Catholique de Louvain, 1973.

УДК 519.7 DOI 10.17223/2226308X/8/5

СВОЙСТВА ГРУППЫ, ПОРОЖДЁННОЙ ГРУППАМИ СДВИГОВ ВЕКТОРНОГО ПРОСТРАНСТВА И КОЛЬЦА ВЫЧЕТОВ

Б. А. Погорелов, М. А. Пудовкина

Аддитивные группы кольца вычетов $\mathbb{Z}_{2^n}$ и векторного пространства V_n над полем GF(2), а также порождённая ими группа G_n имеют общие системы импримитивности и являются подгруппами силовской 2-подгруппы симметрической группы $S(\mathbb{Z}_{2^n})$. Данные группы возникают в криптографии при использовании в качестве способа наложения ключа относительно операций сложения из V_n и $\mathbb{Z}_{2^n}$. В работе приведено подстановочное строение подгрупп группы G_n. Показано, что подгруппами G_n являются группа нижнетреугольных $(n\times n)$-матриц над полем GF(2) и полная аффинная группа над кольцом вычетов $\mathbb{Z}_{2^n}$. Рассмотрена характеризация импримитивных подгрупп группы G_n.

Ключевые слова: *сплетение групп подстановок, импримитивная группа, силовская 2-подгруппа, аддитивная группа кольца вычетов, аддитивная группа векторного пространства, ARX-шифрсистема.*

Аддитивная группа $\mathbb{Z}_{2^n}^+$ кольца вычетов $\mathbb{Z}_{2^n}$ и аддитивная группа V_n^+ n-мерного векторного пространства V_n над полем GF(2), а также порождённая ими группа $G_n = \left\langle V_n^+, \mathbb{Z}_{2^n}^+ \right\rangle$ являются подгруппами силовской 2-подгруппы $P_n \in \mathrm{Syl}_2\left(S_{2^n}\right)$, описываемой операцией сплетения $P_n = P_2 \wr P_{n-1}$. Все эти группы имеют общие системы импримитивности $W^{(i,n)} = \left\{W_0^{(i,n)}, \ldots, W_{2^i-1}^{(i,n)}\right\}$, где

$$W_t^{(i,n)} = \left\{j \in \{0, \ldots, 2^n - 1\} : j \equiv t \,(\mathrm{mod}\ 2^i)\right\},\ i = 1, \ldots, n-1,\ t = 0, \ldots, 2^i - 1.$$

Заметим, что в криптографии группа G_n возникает в блочных шифрсистемах, использующих в качестве наложения ключа сложения в кольце вычетов и в векторном пространстве, например IDEA, ARX. В связи с наличием общих систем импримитивности у групп $\mathbb{Z}_{2^n}^+$, V_n^+ операции сложения $+$, $\oplus$ в кольце вычетов $\mathbb{Z}_{2^n}$ и в векторном пространстве V_n соответственно оказались достаточно близки.

Приведём подстановочное строение подгрупп группы G_n, из описания которого, в частности, следует известный порядок группы G_n, полученный ранее в [1].

Теорема 1. Пусть $n \geqslant 2$. Тогда:

1) если $\varphi_{n-1}^{(G_n)}$ — естественный гомоморфизм импримитивной группы G_n в группу, действующую на множестве блоков импримитивности $\{\{0, 2^{n-1}\}, \ldots, \{2^{n-1} - 1, 2^n - 1\}\}$, то $\mathrm{Im}\varphi_{n-1}^{(G_n)} \cong G_{n-1}$ и

$$\mathrm{Ker}\varphi_{n-1}^{(G_n)} = \Big\langle \Big\{ \big(r, 2^{n-1}+r\big) \cdot \big(2^{n-2}+r, 2^{n-1}+2^{n-2}+r\big) : r = 0, \ldots, 2^{n-2}-1 \Big\}, \prod_{t=0}^{2^{n-2}-1} \big(2^{n-2}+t, 2^{n-1}+2^{n-2}+t\big) \Big\rangle;$$

2) справедливы равенства $\left|\mathrm{Ker}\varphi_{n-1}^{(G_n)}\right| = 2^{2^{n-2}+1}$, $|G_n| = 2^{2^{n-1}+n-1}$.

Пусть $u_{r,n} = (r, 2^{n-1}+r) \cdot (2^{n-2}+r, 2^{n-1}+2^{n-2}+r)$ — произведение транспозиций для $r \in \big\{0, \ldots, 2^{n-2}-1\big\}$.

Опишем нормальные подгруппы группы G_n. Для $n \geqslant 2$ положим

$$R_n^{(j)} = \left\langle \prod_{t=0}^{2^{n-2-j}} u_{r+2^j t(\bmod 2^{n-2}),n} : r \in \big\{0, \ldots, 2^j-1\big\} \right\rangle, j = 0, \ldots, n-2.$$

Заметим, что

$$R_n^{(0)} = Z(G_n),\ \langle e_n \rangle < R_n^{(0)} < R_n^{(1)} < \ldots < R_n^{(n-2)} < \mathrm{Ker}\varphi_{n-1}^{(G_n)},$$
$$\left|R_n^{(j)}\right| = 2^{2^j},\ j = 0, \ldots, n-2,$$

где $Z(G_n)$ — центр группы G_n; e_n — единичный элемент группы G_n.

Утверждение 1. Пусть $n \geqslant 2$. Тогда:

1) $R_n^{(m)} \lhd G_n$ для произвольного $m \in \{0, \ldots, n-2\}$;
2) группа $R_n^{(1)}$ является единственной нормальной подгруппой группы G_n, удовлетворяющей одновременно условиям $|R_n^{(1)}| = 4$, $Z(G_n) < R_n^{(1)} < \mathrm{Ker}\varphi_{n-1}^{(G_n)}$;
3) группа $R_n^{(n-2)}$ является максимальной нормальной подгруппой группы G_n в $\mathrm{Ker}\varphi_{n-1}^{(G_n)}$.

Как следствие теоремы 1 описаны некоторые модулярные представления группы G_n над полем $\mathrm{GF}(2)$.

Доказано, что примитивная группа, подгруппой которой является G_n, совпадает с группой $S(\mathbb{Z}_{2^n})$. Поэтому представляют интерес только импримитивные группы, содержащие G_n и её подгруппы. В частности, для характеризации импримитивных подгрупп группы G_n рассмотрены полная аффинная группа $AGL_1(\mathbb{Z}_{2^n})$ над $\mathbb{Z}_{2^n}$ и группа LT_n нижнетреугольных $(n \times n)$-матриц над полем $\mathrm{GF}(2)$. Доказаны включения $LT_n < G_n$, $GL_1(\mathbb{Z}_{2^n}) < G_n$ для $n \geqslant 2$. Рассмотрено также обратное преобразование s_n над кольцом $\mathbb{Z}_{2^n}$, являющееся аналогом преобразования $x \mapsto x^{-1}$ над полем $\mathrm{GF}(2^n)$, и доказана справедливость включения $s_n \in P_n$ для $n \geqslant 2$.

ЛИТЕРАТУРА

1. *Grossman E.* Group Theoretic Remarks on Cryptographic Systems Based on Two Types of Additions. IBM Report RC-4742, Yorktown Heights, N.Y., Feb. 1974.