ЛИТЕРАТУРА

1. *Merkle R. C. and Hellman M. E.* Hiding information and signatures in trap-door knapsacks // IEEE Trans. Inform. Theory. 1978. V. IT-24. P. 525–530.
2. *Саломаа А.* Криптография с открытым ключом. М.: Мир, 1995. 318 с.

УДК 512.542.74

ОПИСАНИЕ КЛАССА ПОДСТАНОВОК, ПРЕДСТАВИМЫХ В ВИДЕ ПРОИЗВЕДЕНИЯ ДВУХ ПОДСТАНОВОК С ФИКСИРОВАННЫМ ЧИСЛОМ МОБИЛЬНЫХ ТОЧЕК. II

А. Б. Пичкур

Пусть подстановка $G \in S_N$, $\Gamma(G) \subseteq \{1, \ldots, N\}$ — множество мобильных точек подстановки G, $2 \leqslant q \leqslant N$, $\Gamma_N(q) = \{G \in S_N : |\Gamma(G)| = q\}$ — множество всех подстановок степени N, имеющих ровно q мобильных точек.

В предшествующей работе (см. [1]) полностью описано строение множества $\Gamma_N(q) \cdot \Gamma_N(q)$ при $4 \leqslant q \leqslant N/2$ и $N \geqslant 8$.

В данной работе описано множество всех подстановок из $\Gamma_N(q) \cdot \Gamma_N(q+t)$ при $t \geqslant 1$. Этот результат имеет практические приложения в криптографии.

Сначала приведём результаты о строении множества $\Gamma_N(q) \cdot \Gamma_N(q+1)$.

Утверждение 1. Если $N \geqslant 6$, $2 \leqslant q_1 < q_2 < N$, то имеет место включение $\Gamma_N(q_1) \cdot \Gamma_N(q_2) \subseteq \Gamma_N(q_1+1) \cdot \Gamma_N(q_2+1)$.

Теорема 1. Пусть $N \geqslant 8$, $3 \leqslant q \leqslant N/2$, $G \in S_N$. Если $1 < |\Gamma(G)| \leqslant 2q-1$, то существуют подстановки $H_1 \in \Gamma_N(q)$, $H_2 \in \Gamma_N(q+1)$, для которых выполняется равенство $G = H_1 \cdot H_2$.

Далее рассмотрим, какие подстановки из множеств $\Gamma_N(2q+1)$, $\Gamma_N(2q)$ принадлежат произведению $\Gamma_N(q) \cdot \Gamma_N(q+1)$.

Утверждение 2. Пусть $N \geqslant 4$, $2 \leqslant q < N/2$, подстановка $G \in \Gamma_N(2q+1)$ является произведением r неединичных циклов, длины которых равны $m_1, m_2, \ldots, m_r$, $\sum\limits_{i=1}^{r} m_i = 2q+1$. Подстановка G принадлежит множеству $\Gamma_N(q) \cdot \Gamma_N(q+1)$ в том и только в том случае, когда существует такое подмножество $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, r\}$, что $m_{i_1} + \cdots + m_{i_k} = q$.

Утверждение 3. Пусть $N \geqslant 4$, $2 \leqslant q \leqslant N/2$, подстановка $G \in \Gamma_N(2q)$ является произведением r неединичных циклов, длины которых равны $m_1, m_2, \ldots, m_r$, $\sum\limits_{i=1}^{r} m_i = 2q$. Подстановка G принадлежит множеству $\Gamma_N(q) \cdot \Gamma_N(q+1)$ в том и только в том случае, когда выполнено условие: существует $i_0 \in \{1, \ldots, r\}$ и существует такое подмножество $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, r\} \setminus \{i_0\}$, что $m_{i_0} > 2$ и $q - m_{i_1} + m_{i_2} + \cdots + m_{i_k} \in \in \{2, \ldots, m_{i_0} - 1\}$.

Итак, в теореме 1 и утверждениях 2 и 3 полностью описано строение множества $\Gamma_N(q) \cdot \Gamma_N(q+1)$ при $3 \leqslant q \leqslant N/2$.

Наконец, приведем результаты о строении множества $\Gamma_N(q) \cdot \Gamma_N(q+t)$, $t \geqslant 2$.

Теорема 2. Пусть $N > 10$, $2 \leqslant t < N-2$, $2 \leqslant q < (N-t)/2+1$, $G \in S_N$. Если $t \leqslant |\Gamma(G)| \leqslant 2q+t-2$, то существуют подстановки $H_1 \in \Gamma_N(q)$, $H_2 \in \Gamma_N(q+t)$, для которых выполняется равенство $G = H_1 \cdot H_2$.

Можно доказать утверждения, аналогичные утверждениям 2 и 3, которые показывают, какие подстановки из множеств $\Gamma_N(2q+t-1)$, $\Gamma_N(2q+t)$ принадлежат произведению $\Gamma_N(q)\cdot\Gamma_N(q+t)$.

ЛИТЕРАТУРА

1. *Пичкур А. Б.* Описание класса подстановок, представимых в виде произведения двух подстановок с фиксированным числом мобильных точек // Прикладная дискретная математика. Приложение. 2011. №4. С. 16–17.

УДК 519.7

О КОМБИНАТОРНЫХ СВОЙСТВАХ ГРУППЫ, ПОРОЖДЁННОЙ XL-СЛОЯМИ[1]

Б. А. Погорелов, М. А. Пудовкина

Алгоритмы блочного шифрования реализуются итеративным применением более простых преобразований, которые должны обеспечивать свойства перемешивания, рассеивания и усложнения. Для получения данных свойств обычно используются слои преобразований трёх типов: наложение ключа (X-слой), преобразования над отдельными частями блока текста (слой s-боксов) и линейное преобразование (линейный слой, или L-слой). Блочные шифрсистемы с таким построением раундовых преобразований и побитным подмешиванием раундового ключа в каждом раунде называют XSL-сетями. Ряд линейных преобразований, используемых в линейном слое в алгоритмах шифрования и обеспечивающих хорошее рассеивание, являются приводимыми. Естественно, приводимыми являются и характеристические многочлены подстановочных матриц, используемых в SP-сетях. Это приводит к импримитивности подгруппы $C(g)$ аффинной группы $AGL_n(2)$, порождённой слоем наложения раундового ключа (т. е. всеми сдвигами) и приводимой невырожденной матрицей $g\in GL_n(2)$. В данной работе рассматриваются свойства графов орбиталов группы $C(g)$.

Пусть $\mathbb{N}$ — множество всех натуральных чисел; V_n — векторное пространство размерности n над GF(2); $X^\times = X\backslash\{0\}$; $\tilde{g}$ — матрица линейного преобразования g в стандартном базисе $\varepsilon_0,\dots,\varepsilon_{n-1}$, где $\varepsilon_i = (0,...,0,1,\underbrace{0,...,0}_{i})\in V_n$, $i\in\{0,\dots,n-1\}$; GL_n — полная линейная группа; $\chi_g(x)$ — характеристический многочлен линейного преобразования $g\in GL_n(2)$; $m_{\gamma,g}(x)$ — минимальный многочлен вектора $\gamma\in V_n^\times$ относительно преобразования g.

Напомним, что орбиталами группы G, действующей на множестве X, называются орбиты группы G при её действии на множестве X^2. Действие группы G на множестве X^2 задано как $(\alpha,\beta)^f=(\alpha^f,\beta^f)$ для всех $(\alpha,\beta)\in X^2$ и $f\in G$.

Лемма 1. Для произвольного преобразования $g\in GL_n$ и векторов $\alpha,\beta,\alpha',\beta'\in V_n$, $\alpha\neq\beta$, $\alpha'\neq\beta'$, тогда и только тогда $(\alpha',\beta')\in(\alpha,\beta)^{C(g)}$, когда $\alpha'\oplus\beta'\in(\alpha\oplus\beta)^{\langle g\rangle}$.

Таким образом, различными нетривиальными графами орбиталов группы $C(g)$ являются $\bar{\Gamma}_{(\mathbf{0},\gamma_1)}(g),\dots,\bar{\Gamma}_{(\mathbf{0},\gamma_{d-1})}(g)$, где $\gamma_1^{\langle g\rangle},\dots,\gamma_{d-1}^{\langle g\rangle}$ — попарно различные орбиты группы $\langle g\rangle$ на $V_n^\times$. Среди графов орбиталов группы $C(g)$ могут встречаться изоморфные.

Существует тесная связь между строением характеристического многочлена $\chi_g(x)$ преобразования g, примитивностью (2-транзитивностью) и связностью графов орбиталов группы $C(g)$. Так, группа $C(g)$ примитивна тогда и только тогда, когда много-

[1]Работа выполнена при поддержке гранта Президента РФ НШ №6260.2012.10е