Math-Net.Ru

Общероссийский математический портал

Б. А. Погорелов, М. А. Пудовкина, Неабелевость группы наложения ключа и свойство $\otimes \mathbf{w}$ -марковости алгоритмов блочного шифрования, *Матем. вопр. криптогр.*, 2020, том 11, выпуск 4, 107–131

DOI: <https://doi.org/10.4213/mvk343>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 52.6.47.48

26 апреля 2023 г., 10:22:57

Неабелевость группы наложения ключа и свойство $\otimes_{\mathbf{W}}$ -марковости алгоритмов блочного шифрования

Б. А. Погорелов¹, М. А. Пудовкина²

¹Академия криптографии Российской Федерации, Москва

²Московский государственный технический университет
имени Н. Э. Баумана, Москва

Получено 29.IV.2019

Аннотация. Для абелевой группы наложения ключа $(X, \otimes)$ и разбиения $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ множества X авторами рассматривались $\otimes_{\mathbf{W}}$ -марковские преобразования и $\otimes_{\mathbf{W}}$ -марковские алгоритмы. Свойство $\otimes_{\mathbf{W}}$ -марковости связано с различными обобщениями разностного метода. В данной работе описываются свойства $\otimes_{\mathbf{W}}$ -марковских алгоритмов и преобразований для неабелевой группы $(X, \otimes)$. Получены ограничения на строение групп $(X, \otimes)$, $\langle g_k | k \in X \rangle$, а также на блоки $W_0, \dots, W_{r-1}$, вытекающие из условия сохранения частичной раундовой функцией $g_k : X \rightarrow X$ нетривиального разбиения $\mathbf{W}$ для $k \in X$. Для всех неабелевых групп порядка 2^m , обладающих циклической подгруппой индекса два, описаны классы $\otimes_{\mathbf{W}}$ -марковских подстановок.

Ключевые слова: марковский алгоритм блочного шифрования, $\otimes_{\mathbf{W}}$ -марковость, XSL-алгоритм, неабелевы группы, группа диэдра, обобщенная группа кватернионов

Nonabelian key addition groups and $\otimes_{\mathbf{W}}$ -markovian property of block ciphers

B. A. Pogorelov¹, M. A. Pudovkina²

¹Academy of Cryptography of the Russian Federation, Moscow

²Bauman Moscow State Technical University, Moscow

Abstract. For an Abelian key addition group $(X, \otimes)$ and a partition $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ of a set X we had introduced $\otimes_{\mathbf{W}}$ -markovian transformations and $\otimes_{\mathbf{W}}$ -markovian ciphers. The $\otimes_{\mathbf{W}}$ -markovian condition is required to validate different generalizations of differential technique. In this paper, we study $\otimes_{\mathbf{W}}$ -markovian ciphers and transformations on a nonabelian group $(X, \otimes)$. We get restrictions on the structure of groups $(X, \otimes)$, $\langle g_k | k \in X \rangle$ and blocks of a nontrivial partition $\mathbf{W}$ as a consequence

of the condition of partial preservation of $\mathbf{W}$ by the round function $g_k: X \rightarrow X$ for all $k \in X$. For all nonabelian groups of the order 2^m with a cyclic subgroup having index 2 we describe classes of $\otimes_{\mathbf{W}}$ -markovian permutations.

Keywords: Markovian block cipher, $\otimes_{\mathbf{W}}$ -markovian property, XSL-block cipher, nonabelian group, dihedral group, generalized quaternion group

1. Введение

В связи с обоснованием стойкости относительно разностного метода криптоанализа в [1] введено понятие $\otimes$ -марковских (итерационных) алгоритмов блочного шифрования относительно группы $(X, \otimes)$ наложения ключа с алфавитом текстов X , а также с независимыми и равномерно распределенными раундовыми ключами. Авторами в [2] рассмотрено обобщение $\otimes$ -марковских алгоритмов относительно разбиений множества X^2 , в частности относительно разбиения $\mathbf{W}$ множества разностей X , задаваемых операцией $\otimes$. Приведены условия, при которых укрупнение разностей биграмм текстов в случае $\otimes$ -марковского алгоритма дает марковскую последовательность. Алгоритмы с таким свойством названы $\otimes_{\mathbf{W}}$ -марковскими. Свойство $\otimes_{\mathbf{W}}$ -марковости естественным образом формулируется для преобразований.

В данной работе для произвольной неабелевой группы $(X, \otimes)$ с единичным элементом e рассматривается l -раундовый алгоритм блочного шифрования $C_l(\otimes, b)$, у которого частичная раундовая функция $g_k: X \rightarrow X$, определяемая подстановкой $b \in S(X)$, задана условием

$$g_k: x \mapsto (x \otimes k)^b \text{ для всех } (x, k) \in X^2.$$

К данному классу относятся XSL-алгоритмы блочного шифрования, у которых $(X, \otimes)$ — группа наложения ключа, а $b = sh$, где s — преобразование слоя перемешивания (S -боксы), h — преобразование линейного слоя. Заметим, что $\otimes_{\mathbf{W}}$ -марковость алгоритма $C_l(\otimes, b)$ равносильна $\otimes_{\mathbf{W}}$ -марковости преобразования b . В [3] даны условия $\otimes_{\mathbf{W}}$ -марковости алгоритма блочного шифрования $C_l(\otimes, b)$ для абелевой группы наложения ключа $(X, \otimes)$. В настоящей работе описываются свойства $\otimes_{\mathbf{W}}$ -марковских алгоритмов $C_l(\otimes, b)$ и преобразований для неабелевой группы $(X, \otimes)$.

Пусть $(Y, \odot)$ — группа, $v \in S(Y)$, $|Y| < |X|$. Сюръективное отображение $\theta: X \rightarrow Y$, удовлетворяющее условию

$$\theta\left((x \otimes k)^b\right) = (\theta(x) \odot \theta(k))^v \text{ для всех } (x, k) \in X^2,$$

называется гомоморфизмом алгоритма $C_l(\otimes, b)$ в алгоритм $C_l(\odot, v)$ (далее гомоморфизм алгоритма $C_l(\otimes, b)$).

В данной работе установлена связь между существованием гомоморфизма θ и $\otimes_{\mathbf{W}}$ -марковостью алгоритма $C_l(\otimes, b)$ в случае неабелевых групп. Доказано, что наложение на множество $\{g_k | k \in X\}$ условия сохранения разбиения $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ множества X , $e \in W_0$, приводит к существенным ограничениям на разбиение $\mathbf{W}$, а именно блоки разбиения $\mathbf{W}$ суть правые смежные классы группы $(X, \otimes)$ по подгруппе $(W_0, \otimes)$. В этом случае группа $G = \langle g_k | k \in X \rangle$ импримитивна, а алгоритм $C_l(\otimes, b)$ является $\otimes_{\mathbf{W}}$ -марковским.

Из импримитивности группы G также вытекает существование подстановочного гомоморфизма $\tilde{\varphi}_{\mathbf{W}}$ — естественного гомоморфизма импримитивной группы G в симметрическую группу, действующую на множестве блоков $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$. Этот гомоморфизм однозначно определяется отображением $\varphi_{\mathbf{W}} : X \rightarrow \{0, \dots, r-1\}$, заданным условием $\varphi_{\mathbf{W}} : \alpha \mapsto i$, если $\alpha \in W_i$, $i \in \{0, \dots, r-1\}$. Подстановочный гомоморфизм $\tilde{\varphi}_{\mathbf{W}}$ связан с отображением $\varphi_{\mathbf{W}}$ равенством

$$(\varphi_{\mathbf{W}}(\alpha))^{\tilde{\varphi}_{\mathbf{W}}(b)} = \varphi_{\mathbf{W}}(\alpha^b) \text{ для всех } (\alpha, b) \in X \times G.$$

В общем случае из наличия подстановочного гомоморфизма $\tilde{\varphi}_{\mathbf{W}}$ группы G не следует существование гомоморфизма θ алгоритма $C_l(\otimes, b)$. В случае $(W_0, \otimes) \triangleleft (X, \otimes)$ доказана эквивалентность между $\otimes_{\mathbf{W}}$ -марковостью алгоритма $C_l(\otimes, b)$, существованием нетривиального подстановочного гомоморфизма $\tilde{\varphi}_{\mathbf{W}}$ группы G , а также существованием гомоморфизма θ алгоритма $C_l(\otimes, b)$. Рассмотрены «простейшие» неабелевы группы порядка 2^m , потенциально представляющие интерес для практического применения. Из теоремы 12.5.1 [5] следует, что неабелевы группы $(X, \otimes)$ порядка 2^m , обладающие циклической подгруппой индекса два, могут быть только следующих типов.

- 1) Группа диэдра D_{2^m} , $m \geq 3$, с образующими элементами u , a и определяющими соотношениями

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

- 2) Обобщенная группа кватернионов Q_{2^m} , $m \geq 3$, с образующими элементами u , a и определяющими соотношениями

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

- 3) Модулярная максимально-циклическая группа M_{2^m} , $m \geq 4$, с образующими элементами u , a и определяющими соотношениями

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

- 4) Полудиэдральная (или квазидиэдральная) группа SD_{2^m} , $m \geq 4$, с образующими элементами u , a и определяющими соотношениями

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

Для этих четырех групп приведены примеры таких $\otimes_{\mathbf{W}}$ -марковских алгоритмов, что $(W_0, \otimes) \not\triangleleft (X, \otimes)$, $e \in W_0$, отображение $\varphi_{\mathbf{W}}$ не задает гомоморфизм алгоритма $C_l(\otimes, b)$. Кроме того, описаны разбиения $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ и подстановки b , для которых алгоритм $C_l(\otimes, b)$ является $\otimes_{\mathbf{W}}$ -марковским. Отображение $\varphi_{\mathbf{W}}$ определяет (изоморфное) вложение группы $G = \langle b, X^{\otimes} \rangle$ в $S_{2^{m-1}}$, где $X^{\otimes}$ — регулярное подстановочное представление группы $(X, \otimes)$,

$$X^{\otimes} = \langle \sigma_k : x \mapsto x \otimes k | k \in X \rangle.$$

2. Основные обозначения и понятия

В работе используются следующие обозначения: X — произвольное непустое конечное множество; $(X, \otimes)$ — группа на множестве X с бинарной операцией $\otimes$ и единичным элементом e_X ; если множество X однозначно определено из контекста, то полагаем $e = e_X$; $X^{\times} = X \setminus \{e\}$; $\alpha^b = \alpha b = b(\alpha)$ — образ элемента $\alpha \in X$ при действии на него подстановкой $b \in S(X)$; α^{-1} — обратный к α элемент относительно операции $\otimes$, $\alpha \otimes \beta^{-1} = \alpha \bar{\otimes} \beta$ для любых $\alpha, \beta \in X$; $I(A)$ — индикатор выполнения условия A ; K — множество всех раундовых ключей; $K = X$; $g: X \times K \rightarrow X$ — раундовая функция, а $g_k: \alpha \mapsto g(\alpha, k)$ — частичная раундовая функция, $(\alpha, k) \in X \times K$; $B^b = \{\alpha^b | \alpha \in B\}$ для $B \subseteq X$, $b \in S(X)$; $(H, \otimes) \trianglelefteq (X, \otimes)$ — нормальность подгруппы $(H, \otimes)$ в группе $(X, \otimes)$; $\langle b \rangle$ — циклическая группа, порожденная подстановкой $b \in S(X)$; $W^{(b)} = \{\lambda^g | (\lambda, g) \in W \times \langle b \rangle\}$ для $W \subseteq X$, $b \in S(X)$; $X : H$ — множество смежных классов группы $(X, \otimes)$ по подгруппе $(H, \otimes)$; $|X : H|$ — индекс подгруппы $(H, \otimes)$ в группе $(X, \otimes)$; $\|\alpha\|_2$ — логарифмическая норма элемента $\alpha \in \mathbb{N}$, т. е. $\alpha = 2^{\|\alpha\|_2} \beta$, $2 \nmid \beta$.

Пусть $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ — разбиение множества X на r блоков $W_0, \dots, W_{r-1}$ (см., например, [9]). Положим $\mathbf{W}^b = \{W_0^b, \dots, W_{r-1}^b\}$ для $b \in S(X)$.

Для $b \in S(X)$ и $\theta, \varepsilon \in X$ положим

$$p_{\theta, \varepsilon}(g) = |\{(\alpha, k) \in X \times K \mid (\theta \otimes \alpha)^{gk} = \varepsilon \otimes \alpha^{gk}\}| |K|^{-1} |X|^{-1},$$

$$p_{\theta, \varepsilon}(g|\beta) = |K|^{-1} |\{k \in K \mid (\theta \otimes \beta)^{gk} = \varepsilon \otimes \beta^{gk}\}|, \quad \beta \in X,$$

$$\hat{p}_{\theta, \varepsilon}(b) = |X|^{-1} \left| \left\{ \alpha \in X \mid (\theta \otimes \alpha)^b = \varepsilon \otimes \alpha^b \right\} \right|,$$

$\mathbf{p}(g) = (p_{\theta, \varepsilon}(g))$ — усредненная по ключам матрица вероятностей переходов (разностей) частичной раундовой функции g , а $\hat{\mathbf{p}}(b) = (\hat{p}_{\theta, \varepsilon}(b))$ — матрица вероятностей переходов разностей преобразования b .

Рассмотрим произвольную дискретную однородную цепь Маркова $\zeta^{(0)}, \zeta^{(1)}, \dots$ с конечным множеством состояний Q и матрицей вероятностей переходов $\mathbf{q} = (q_{i,j})$. Для произвольного разбиения $\mathbf{U} = \{U_0, \dots, U_{r-1}\}$ множества состояний Q определим такую последовательность дискретных случайных величин $\zeta_{\mathbf{U}}^{(0)}, \zeta_{\mathbf{U}}^{(1)}, \dots, \zeta_{\mathbf{U}}^{(l)}, \dots$ на множестве $\{0, \dots, r-1\}$, что $\zeta_{\mathbf{U}}^{(t)} = j$ тогда и только тогда, когда $\zeta^{(t)} \in U_j$ для каждого $j \in \{0, \dots, r-1\}$, $t = 0, 1, \dots$

Определение 1 ([4]). Будем говорить, что состояния цепи Маркова можно укрупнить посредством разбиения $\mathbf{U}$, если для каждого распределения случайной величины $\zeta^{(0)}$ на множестве Q последовательность случайных величин $\zeta_{\mathbf{U}}^{(0)}, \zeta_{\mathbf{U}}^{(1)}, \dots, \zeta_{\mathbf{U}}^{(l)}$ является цепью Маркова, переходные вероятности которой не зависят от распределения случайной величины $\zeta^{(0)}$. Полученную цепь Маркова будем называть укрупненной.

Определение 2 ([1]). Алгоритм блочного шифрования с раундовой функцией g и с независимыми и равновероятно выбираемыми раундовыми ключами называется $\otimes$ -марковским, если для всех элементов $\theta, \varepsilon \in X^\times$, $\alpha \in X$ выполняется равенство

$$p_{\theta, \varepsilon}(g|\alpha) = p_{\theta, \varepsilon}(g). \quad (1)$$

Другими словами, вероятности в (1) не зависят от блока текста α при случайном равновероятном выборе раундового ключа из множества K .

Известно (см. [1]), что для $\otimes$ -марковского алгоритма шифрования с раундовой функцией g и любой дискретной случайной величины $\xi^{(0)}$ на множестве X последовательность случайных величин

$$\xi^{(t)} = (\xi^{(0)} \otimes \alpha)^{g_{k_1} \dots g_{k_t}} \bar{\otimes} \alpha^{g_{k_1} \dots g_{k_t}}, \quad t = 1, \dots, l,$$

является цепью Маркова для каждого $\alpha \in X$, где раундовые ключи $k_1, \dots, k_l$ независимо и равновероятно выбираемы из множества K .

Определение 3 ([2]). Назовем l -раундовый итерационный $\otimes$ -марковский алгоритм блочного шифрования с марковской последовательностью $\xi^{(0)}, \dots, \xi^{(l)}$ $\otimes_{\mathbf{W}}$ -марковским для разбиения $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$, $r \geq 2$, если последовательность случайных величин $\xi_{\mathbf{W}}^{(0)}, \dots, \xi_{\mathbf{W}}^{(l)}$ является цепью Маркова.

Определение 4. Разбиение $\{\{\alpha\} | \alpha \in X\}$ множества X называется тривиальным. Разбиение $\mathbf{W}$ множества X нетривиально, если $\mathbf{W} \notin \{\{\{\alpha\} | \alpha \in X\}, \{X\}\}$.

Зафиксируем произвольное нетривиальное разбиение $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ множества X . Положим

$$p_{\theta, W_c}(g) = \sum_{\theta' \in W_c} p_{\theta, \theta'}(g), \theta \in X, c \in \{0, \dots, r-1\}.$$

В [2] (утверждение 3) доказано, что тогда и только тогда $\otimes$ -марковский алгоритм шифрования является $\otimes_{\mathbf{W}}$ -марковским, когда $p_{\theta, W_c}(g) = a_{j,c}$ для каждого $(j, c) \in \{0, \dots, r-1\}^2$, $\theta \in W_j$ и некоторых $a_{j,c}$, $0 \leq a_{j,c} \leq 1$.

Пусть g — раундовая функция $\otimes_{\mathbf{W}}$ -марковского алгоритма блочного шифрования; поставим ей в соответствие матрицу $\mathbf{p}_{\mathbf{W}}(g) = (p_{W_j, W_c}(g))$ вероятностей переходов блоков, где $p_{W_j, W_c}(g) = a_{j,c}$ для $(j, c) \in \{0, \dots, r-1\}^2$.

Для разбиения $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ и преобразования $b \in S(X)$ положим

$$\hat{p}_{\theta, W_c}(b) = \sum_{\theta' \in W_c} \hat{p}_{\theta, \theta'}(b), \quad \theta \in X, c \in \{0, \dots, r-1\}.$$

Определение 5 ([2]). Преобразование $b \in S(X)$ назовем $\otimes_{\mathbf{W}}$ -марковским для разбиения $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$, $|X| \geq r \geq 2$, если $\hat{p}_{\theta, W_c}(b) = a_{j,c}$ для каждого $(j, c) \in \{0, \dots, r-1\}^2$, $\theta \in W_j$ и некоторых $a_{j,c}$, $0 \leq a_{j,c} \leq 1$.

Рассмотрим также матрицу $\hat{\mathbf{p}}_{\mathbf{W}}(b) = (\hat{p}_{W_j, W_c}(b))$ для $\otimes_{\mathbf{W}}$ -марковского преобразования b , где

$$\hat{p}_{W_j, W_c}(b) = \hat{p}_{\theta, W_c}(b) = a_{j,c}$$

для каждого $(j, c) \in \{0, \dots, r-1\}^2$, $\theta \in W_j$ и некоторых $a_{j,c}$, $0 \leq a_{j,c} \leq 1$.

Преобразование $b \in S(X)$ и $\otimes$ -марковский алгоритм блочного шифрования являются $\otimes_{\mathbf{W}}$ -марковскими, если разбиение $\mathbf{W}$ множества X

тривиально или равно $\{\{e\}, X^\times\}$. Поэтому далее в работе рассматриваются разбиения множества X , которые отличны от тривиального и $\{\{e\}, X^\times\}$.

Будем говорить, что множество $Q \subseteq S(X)$ сохраняет (в целом) разбиение $\mathbf{W}$ множества X , если $W^q \in \mathbf{W}$ для всех $(W, q) \in \mathbf{W} \times Q$.

Обозначим через $\text{IG}_{\mathbf{W}}$ максимальную подгруппу группы $S(X)$, сохраняющую в целом разбиение $\mathbf{W}$ множества X , т. е.

$$\text{IG}_{\mathbf{W}} = \{b \in S(X) | \mathbf{W}^b = \mathbf{W}\}.$$

Определение 6. Подстановочным гомоморфизмом будем называть естественный гомоморфизм $\varphi_{\mathbf{W}}^{(G)}$ импримитивной группы G с системой импримитивности $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ в симметрическую группу $S(\{0, \dots, r-1\})$.

Определение 7. Пусть Y — произвольное конечное множество. Укрупнением разбиения $\mathbf{W} = \{W_0, \dots, W_{d-1}\}$ множества Y называется разбиение $\mathbf{W}' = \{W'_0, \dots, W'_{r-1}\}$, блоки которого являются укрупнением блоков разбиения $\mathbf{W}$, т. е. $W'_c = \bigcup_{i \in J_c} W_i$ для некоторого разбиения $J = \{J_0, \dots, J_{r-1}\}$ множества $\{0, \dots, d-1\}$.

3. Гомоморфизмы алгоритма $C_1(\otimes, b)$

и $\otimes_{\mathbf{W}}$ -марковость

В данном разделе для произвольной группы $(X, \otimes)$ и подстановки $b \in S(X)$ рассматривается класс алгоритмов $C_l(\otimes, b)$. Заметим, что к данному классу относятся XSL-алгоритмы блочного шифрования, у которых $b = sh$, где s — преобразование слоя перемешивания (S -боксы), h — преобразование линейного слоя.

Рассмотрим преобразование $\sigma_k \in S(X)$, заданное условием

$$\sigma_k : x \mapsto x \otimes k \text{ для каждого } k \in X,$$

и группу $X^\otimes = \langle \sigma_k | k \in X \rangle$. Далее $X^\otimes$ будем называть группой сдвигов, что принято, например, в квантовом криптоанализе.

Пусть $\rho : X \rightarrow S(X)$ — правое регулярное представление группы $(X, \otimes)$. Очевидно, что

$$\rho(X) = X^\otimes, \quad \rho(k) = \sigma_k, \quad g_k = \sigma_k b \text{ для каждого } k \in X.$$

Всюду далее

$$G = \langle g_k | k \in X \rangle = \langle b, X^\otimes \rangle.$$

Предположим, что существует нетривиальное разбиение $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ множества X , где $e \in W_0$, $r \geq 2$, сохраняемое множеством $\{g_k | k \in X\}$. Укажем ограничения на группы X , G , а также на блоки $W_0, \dots, W_{r-1}$, вытекающие из условия инвариантности разбиения $\mathbf{W}$ относительно множества $\{g_k | k \in X\}$. Заметим, что для алгоритма $C_l(\otimes, b)$ справедливо равенство

$$\hat{\mathbf{p}}(b) = \mathbf{p}(g).$$

Утверждение. Пусть $G = \langle g_k | k \in X \rangle$, существует такое нетривиальное разбиение $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ множества X , что $e \in W_0$, $r \geq 2$ и множество $\{g_k | k \in X\}$ сохраняет разбиение $\mathbf{W}$. Тогда справедливы следующие утверждения.

- 1) Группа G импримитивна с системой импримитивности $\mathbf{W}$, и $w = |W_0| = \dots = |W_{r-1}|$ для некоторого $w \in \mathbb{N}$, $1 < w < |X|$.
- 2) $(W_0, \otimes) \leq (X, \otimes)$, а W_j — j -й правый смежный класс группы $(X, \otimes)$ по $(W_0, \otimes)$ для $j = 0, \dots, r-1$.
- 3) Если группа G не имеет точных подстановочных представлений степени d , где $d \mid |X|$, $d < |X|$, а среди всех нетривиальных разбиений, сохраняемых G , блоки разбиения $\mathbf{W}$ имеют минимальную мощность, то $(W_0, \otimes) \triangleleft (X, \otimes)$.

Доказательство. Так как для произвольных элементов $k_1, k_2 \in X$ подстановки g_{k_1}, g_{k_2} сохраняют разбиение $\mathbf{W}$, то подстановка

$$g_{k_1} g_{k_2}^{-1} = \sigma_{k_1} b b^{-1} \sigma_{k_2}^{-1} = \sigma_{k_1 \otimes k_2},$$

а потому и группа $X^\otimes$ также сохраняют разбиение $\mathbf{W}$. Кроме того, $\mathbf{W}^{g_e} = \mathbf{W}^b = \mathbf{W}$. Поэтому группа G сохраняет разбиение $\mathbf{W}$. Далее доказательства пп. 1 и 2 следуют из утверждения 17 главы 24 [11].

Для доказательства п. 3 достаточно показать, что $(W_0, \otimes) \triangleleft (X, \otimes)$, если группа G не имеет точных подстановочных представлений степени d , где $d \mid |X|$, $d < |X|$. Группа G сохраняет разбиение на смежные классы по подгруппе W_0 , являющееся также системой импримитивности. Поэтому имеется естественный гомоморфизм φ группы G в группу подстановок меньшей степени. Согласно п. 3 условия утверждения 3 не существует точных представлений меньшей степени. Поэтому $\text{Ker} \varphi$ нетривиально.

Очевидно, что орбиты подгруппы $\text{Ker} \varphi$ группы G равномощны и задают разбиение множества X , сохраняемое группой G . Пусть $w' -$

длина произвольной орбиты $\text{Кег}\varphi$. Если $w' < |W_0|$, то возникает противоречие с тем, что блоки разбиения $\mathbf{W}$ имеют наименьшую мощность среди нетривиальных разбиений, сохраняемых группой G . Поэтому $w' = |W_0|$. Значит, $\langle \sigma_k | k \in W_0 \rangle = X^\otimes \cap \text{Кег}\varphi$. Следовательно, $(W_0, \otimes) \triangleleft (X, \otimes)$. $\square$

Заметим, что из импримитивности группы G следуют включения:

$$b \in \text{IG}_{\mathbf{W}}, \quad G \leq \text{IG}_{\mathbf{W}}, \quad \langle g_{k^{(1)}} \dots g_{k^{(l)}} | (k^{(1)}, \dots, k^{(l)}) \in X^l \rangle \leq \text{IG}_{\mathbf{W}}.$$

Однако если группа $G = \langle b, X^\otimes \rangle$ примитивна, то множество $\{g_k | k \in X\}$ не сохраняет никакое нетривиальное разбиение множества X .

Приведем пример неабелевой группы X и разбиения $\mathbf{W}$, удовлетворяющих п. 3 утверждения 3. Пусть p – простое нечетное число, $X^\otimes$ – группа диэдра порядка $2p$. Группа $X^\otimes$ импримитивна с единственной системой импримитивности $\mathbf{W} = \{W_0, W_1\}$, $|W_0| = |W_1| = p$. Группа G совпадает со сплетением $S_p \wr S_2$, например если b – транспозиция, действующая на одном из блоков $W \in \mathbf{W}$. Заметим, что блоки мощности p являются блоками наименьшей мощности, сохраняемыми группой G . Кроме того, G не имеет точных подстановочных представлений меньшей степени. Таким образом, $(X, \otimes)$ – неабелева группа, удовлетворяющая условиям п. 3 утверждения 3.

Пусть $(X, \otimes)$ – группа Гамильтона (неабелева группа, содержащая только нормальные подгруппы). Известно (см. теорему 12.5.4 [5]), что группа Гамильтона представима как прямое произведение группы кватернионов Q_8 , абелевой группы, каждый элемент которой конечного нечетного порядка, и абелевой группы показателя два.

Пусть $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ – разбиение множества X , W_j – j -й правый смежный класс группы $(X, \otimes)$ по подгруппе $(W_0, \otimes)$ для $j = 0, \dots, r-1$. Рассмотрим отображение $\varphi_{\mathbf{W}} : X \rightarrow \{0, \dots, r-1\}$, заданное условием $\varphi_{\mathbf{W}} : \alpha \mapsto i$ тогда и только тогда, когда $\alpha \in W_i$ для каждого $i \in \{0, \dots, r-1\}$.

Зададим на множестве $\{0, \dots, r-1\}$ бинарную операцию $\odot$ условием

$$W_i \otimes W_j = W_{i \odot j} \text{ для всех } i, j \in \{0, \dots, r-1\}. \quad (2)$$

Очевидно, что бинарная операция $\odot$ корректно определена тогда и только тогда, когда $(W_0, \otimes) \triangleleft (X, \otimes)$ (см., например, [10]). Ясно, что в этом случае справедливо равенство

$$\varphi_{\mathbf{W}}(\alpha \otimes k) = \varphi_{\mathbf{W}}(\alpha) \odot \varphi_{\mathbf{W}}(k), \quad (\alpha, k) \in X^2. \quad (3)$$

Для $b \in \text{IG}_{\mathbf{W}}$ зададим подстановку $\bar{b} \in S(\{0, \dots, r-1\})$ условием

$$(\varphi_{\mathbf{W}}(\alpha))^{\bar{b}} = \varphi_{\mathbf{W}}(\alpha^b) \quad \text{для каждого } \alpha \in X. \quad (4)$$

Нормальность позволяет говорить о замкнутости классов алгоритмов вида $C_l(\otimes, b)$ относительно применения к его элементам подстановочных гомоморфизмов. Очевидно, что условию нормальности W_0 в X удовлетворяют любая абелева группа X и ее подгруппа W_0 .

В следующей теореме показано, что условие $\otimes_{\mathbf{W}}$ -марковости алгоритма $C_l(\otimes, b)$ эквивалентно существованию у него подстановочного гомоморфизма, если $(W_0, \otimes) \triangleleft (X, \otimes)$. Тем самым возникает особый интерес к изучению такого множества алгоритмов. Заметим, что $\otimes_{\mathbf{W}}$ -марковость алгоритма $C_l(\otimes, b)$ равносильна $\otimes_{\mathbf{W}}$ -марковости подстановки b .

Теорема 1. Пусть $l \in \mathbb{N}$, $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ — нетривиальное разбиение множества X , $e \in W_0$, $(W_0, \otimes) \trianglelefteq (X, \otimes)$, $b \in \text{IG}_{\mathbf{W}}$. Тогда следующие условия эквивалентны.

- 1) Разбиение $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ сохраняется множеством $\{g_k | k \in X\}$.
- 2) На множестве $\{0, \dots, r-1\}$ корректно определены бинарная операция $\odot$ и подстановка $\bar{b}$, заданные соответственно условиями 2 и 4, а $\varphi_{\mathbf{W}}$ — гомоморфизм $C_l(\otimes, b)$ в $C_l(\odot, \bar{b})$.
- 3) $C_l(\otimes, b)$ является $\otimes_{\mathbf{W}}$ -марковским, если $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ — множество смежных классов группы $(X, \otimes)$ по ее нормальной подгруппе $(W_0, \otimes)$.

Доказательство. $1 \Rightarrow 2$. Пусть $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ — нетривиальное разбиение множества X , сохраняемое $\{g_k | k \in X\}$. Тогда из утверждения 3 вытекает, что W_j — j -й правый смежный класс группы $(X, \otimes)$ по $(W_0, \otimes)$ для $j = 0, \dots, r-1$. Так как $(W_0, \otimes) \trianglelefteq (X, \otimes)$, то в $C_l(\odot, \bar{b})$ корректно определены бинарная операция $\odot$ и подстановка $\bar{b}$, заданные соответственно условиями (2) и (4). Потому существует алгоритм $C_l(\odot, \bar{b})$, у которого раундовая функция $\bar{g} : \{0, \dots, r-1\}^2 \rightarrow \{0, \dots, r-1\}$ удовлетворяет равенствам

$$\begin{aligned} \bar{g}_{\varphi_{\mathbf{W}}(k)}(\varphi_{\mathbf{W}}(\alpha)) &= \varphi_{\mathbf{W}}(g_k(\alpha)) = \varphi_{\mathbf{W}}((\alpha \otimes k)^b) \\ &= (\varphi_{\mathbf{W}}(\alpha \otimes k))^{\bar{b}} = (\varphi_{\mathbf{W}}(\alpha) \odot \varphi_{\mathbf{W}}(k))^{\bar{b}} \end{aligned} \quad (5)$$

для всех $(\alpha, k) \in X^2$. Из цепочки равенств (5) вытекает, что $\varphi_{\mathbf{W}}$ — гомоморфизм $C_l(\otimes, b)$ в $C_l(\odot, \bar{b})$.

$2 \Rightarrow 3$. Пусть в $C_l(\odot, \bar{b})$ корректно определены бинарная операция $\odot$ и подстановка $\bar{b}$, заданные соответственно условиями (2) и (4), а $\varphi_{\mathbf{W}}$ — гомоморфизм $C_l(\otimes, b)$ в $C_l(\odot, \bar{b})$. Тогда $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ — множество смежных классов группы $(X, \otimes)$ по ее нормальной подгруппе $(W_0, \otimes)$. Так как $b \in \text{IG}_{\mathbf{W}}$ и для каждого $c, j \in \{0, \dots, r-1\}$, $\theta \in W_c$ выполняется равенство $\theta \otimes W_j = W_{c \odot j}$, то для каждого $\beta \in W_j$ и некоторого $u_{c,j} \in \{0, \dots, r-1\}$ справедливы соотношения

$$(\theta \otimes W_j)^b \bar{\otimes} W_j^b = W_{u_{c,j}}, \quad (\theta \otimes \beta)^b \bar{\otimes} \beta^b \in W_{u_{c,j}},$$

из которых для каждого $t \in \{0, \dots, r-1\}$ вытекает равенство

$$\begin{aligned} p_{\theta, W_t}(g) &= r^{-1} \sum_{i=0}^{r-1} \text{I} \left((\theta \otimes W_i)^b \bar{\otimes} W_i^b = W_t \right) \\ &= r^{-1} \sum_{i=0}^{r-1} \text{I} (W_{c \odot i}^b = W_t \otimes W_i^b) \\ &= r^{-1} \sum_{i=0}^{r-1} \text{I} \left((c \odot i)^{\bar{b}} = t \odot i^{\bar{b}} \right) = p_{c,t}(\bar{g}). \end{aligned} \quad (6)$$

Из цепочки равенств (6) и утверждения 3 [2] следует $\otimes_{\mathbf{W}}$ -марковость алгоритма $C_l(\otimes, b)$.

$3 \Rightarrow 1$. Пусть $C_l(\otimes, b)$ является $\otimes_{\mathbf{W}}$ -марковским, где $\mathbf{W}$ — множество смежных классов группы $(X, \otimes)$ по ее нормальной подгруппе $(W_0, \otimes)$. Так как $p_{e, W_0}(g) = 1$, то из утверждения 3 [2] вытекает равенство $p_{\theta, W_0}(g) = 1$ для каждого $\theta \in W_0$, которое для каждого $\alpha \in X$ равносильно

$$(W_0 \otimes \alpha)^b = (\alpha \otimes W_0)^b = W_0^{g_\alpha} = \alpha^b \otimes W_0 = W_0 \otimes \alpha^b.$$

Значит, множество $\{g_k | k \in X\}$ сохраняет разбиение $\mathbf{W}$. $\square$

Приведем пример неабелевых групп, удовлетворяющих теореме 1.

Пример. Пусть $(X, \otimes)$ — группа Гамильтона (неабелева группа, содержащая только нормальные подгруппы). Известно (см. [5, теорема 12.5.4]), что группа Гамильтона представима как прямое произведение группы кватернионов Q_8 , абелевой группы, каждый элемент которой конечного нечетного порядка, и абелевой группы показателя два. Рассмотрим произвольную подгруппу $(W_0, \otimes)$ группы Гамильтона $(X, \otimes)$ и разбиение $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$, состоящее из всех правых смежных классов группы $(X, \otimes)$ по подгруппе $(W_0, \otimes)$. Из теоремы 1 следует,

что $\varphi_{\mathbf{W}}$ задает гомоморфизм $C_l(\otimes, b)$ в $C_l(\odot, \bar{b})$, если $b \in \text{IG}_{\mathbf{W}}$. Данным свойством, например, обладает группа кватернионов Q_8 , так как каждая ее подгруппа нормальна.

Пусть группа $(X, \otimes)$ является декартовым произведением групп $(H_1, \otimes_1), \dots, (H_c, \otimes_c)$. Известно (см., например, [6]), что группа

$$(X, \otimes) = \prod_{i=1}^c (H_i, \otimes_i)$$

неабелева, если неабелева хотя бы одна из групп $(H_1, \otimes_1), \dots, (H_c, \otimes_c)$. Очевидно, что $(H_i, \otimes_i) \trianglelefteq (X, \otimes)$ для $i = 1, \dots, c$. Отсюда вытекает существование такого разбиения $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$, что $(W_0, \otimes) \trianglelefteq (X, \otimes)$, W_j — j -й смежный класс группы $(X, \otimes)$ по подгруппе $(W_0, \otimes)$. Таким образом, из теоремы 1 следует существование таких разбиений $\mathbf{W}$ группы $(X, \otimes)$, что $\varphi_{\mathbf{W}}$ задает гомоморфизм $C_l(\otimes, b)$ в $C_l(\odot, \bar{b})$, если $b \in \text{IG}_{\mathbf{W}}$.

4. $\otimes_{\mathbf{W}}$ -марковские подстановки и неабелевы группы порядка 2^m , обладающие циклической подгруппой индекса два

Для каждой неабелевой группы H_m порядка 2^m , обладающей циклической подгруппой индекса два, в данном разделе опишем класс $\otimes_{\mathbf{W}}$ -марковских подстановок, где $\mathbf{W}$ — множество всех правых смежных классов группы H_m по ее некоторой ненормальной подгруппе. Для групп D_{2^m} , Q_{2^m} , M_{2^m} , SD_{2^m} удобно использовать обозначение $\otimes = \cdot$. Далее понадобится следующая лемма.

Лемма 1 ([7]). Пусть:

- 1) разбиение $\mathbf{W} = \{W_0, \dots, W_{d-1}\}$ множества X и подстановка $b \in S(X)$ таковы, что $\hat{\mathbf{p}}_{\mathbf{W}}(b)$ — подстановочная матрица некоторой подстановки $s \in S(\{0, \dots, d-1\})$,
- 2) $\mathbf{J} = \{J_0, \dots, J_{r-1}\}$ — нетривиальное разбиение множества $\{0, \dots, d-1\}$, а $\mathbf{W}' = \{W'_0, \dots, W'_{r-1}\}$ — укрупнение разбиения $\mathbf{W}$, где

$$W'_i = \bigcup_{j \in J_i} W_j \text{ для } i = 0, \dots, r-1.$$

Подстановка b является $\otimes_{\mathbf{W}'}$ -марковской тогда и только тогда, когда $J_i^s = J_c$ или $J_i^s \cap J_c = \emptyset$ для любых $i, c \in \{0, \dots, r-1\}$. В этом случае $\hat{\mathbf{p}}_{\mathbf{W}'}(b)$ — также подстановочная матрица.

Для произвольной неабелевой группы $(X, \otimes)$ наложения ключа класс разбиений $\mathbf{W}$ множества X , относительно которых подстановка $b \in S(X)$ является $\otimes_{\mathbf{W}}$ -марковской, может быть найден с помощью следующей леммы.

Лемма 2. Пусть $(X, \otimes)$ — произвольная неабелева группа, $b \in S(X)$ и существует такое нетривиальное разбиение $\mathbf{W}$ множества X , что матрица $\hat{\mathbf{p}}_{\mathbf{W}}(b)$ подстановочная. Тогда b — $\otimes_{\mathbf{W}}$ -марковская подстановка. Кроме того, b — $\otimes_{\mathbf{U}}$ -марковская подстановка для каждого укрупнения $\mathbf{U}$ разбиения $\mathbf{W}$, удовлетворяющего лемме 1.

Доказательство. Так как $\hat{\mathbf{p}}_{\mathbf{W}}(b)$ — подстановочная матрица, то для всех $(W, T) \in \mathbf{W}^2$ и всех $(\theta, \theta') \in W^2$ справедливо равенство

$$\hat{p}_{\theta, T}(b) = \hat{p}_{\theta', T}(b) = \hat{p}_{W, T}(b).$$

Отсюда и из определения (4) следует $\otimes_{\mathbf{W}}$ -марковость подстановки b . $\square$

Для каждой из групп $D_{2^m}, Q_{2^m}, M_{2^m}, \text{SD}_{2^m}$ опишем сначала классы подгрупп, которые не являются нормальными.

Положим

$$C(H_m) = \begin{cases} \{0, \dots, 2^{m-1} - 1\}, & \text{если } H_m \in \{D_{2^m}, Q_{2^m}, \text{SD}_{2^m}\}, \\ \{0, 2^{m-2}\}, & \text{если } H_m = M_{2^m}. \end{cases}$$

Лемма 3. Пусть $m \geq 4$, $H_m \in \{D_{2^m}, Q_{2^m}, M_{2^m}, \text{SD}_{2^m}\}$, $H_m = \langle u, a \rangle$, $\text{ord}(a) = 2^{m-1}$, $\text{ord}(u) \in \{2, 4\}$. Тогда и только тогда $\langle ua^c \rangle \not\leq H_m$, когда $c \in C(H_m)$. Кроме того,

$$\text{ord}(ua^c) = \begin{cases} 2, & \text{если } H_m \in \{D_{2^m}, M_{2^m}\} \text{ или } H_m = \text{SD}_{2^m}, c \equiv 0 \pmod{2}, \\ 4, & \text{если } H_m = Q_{2^m} \text{ или } H_m = \text{SD}_{2^m}, c \equiv 1 \pmod{4}. \end{cases}$$

Доказательство. Пусть H_m — группа диэдра D_{2^m} . Очевидно, что $\langle ua^c \rangle$ — подгруппа порядка два для каждого $c \in \{0, \dots, 2^{m-1} - 1\}$.

Зафиксируем $c \in \{0, \dots, 2^{m-1} - 1\}$ и рассмотрим $W_0^{(c)} = \{e, ua^c\}$. Тогда $\mathbf{W}^{(c)} = \{W_0^{(c)}, \dots, W_{2^{m-1}-1}^{(c)}\}$ — множество всех правых смежных классов по подгруппе $W_0^{(c)}$, где $W_j^{(c)} = \{a^j, ua^{j+c}\}$ для $j = 0, \dots, 2^{m-1} - 1$. Заметим, что $\mathbf{U}^{(c)} = \{U_0^{(c)}, \dots, U_{2^{m-1}-1}^{(c)}\}$ — множество всех левых смежных классов, где $U_j^{(c)} = \{a^j, ua^{c-j}\}$ для

$j = 0, \dots, 2^{m-1} - 1$. Так как $\mathbf{W}^{(c)} \neq \mathbf{U}^{(c)}$ для каждого $c \in \{0, \dots, 2^{m-2}\}$, то

$$W_0^{(c)} = \{e, ua^c\} = \langle ua^c \rangle$$

не является нормальной.

Пусть H_m — обобщенная группа кватернионов Q_{2^m} . Рассмотрим подгруппы группы Q_{2^m} порядка четыре

$$W_0^{(c)} = \langle ua^c \rangle = \{e, ua^c, a^{2^{m-2}}, ua^{2^{m-2}+c}\} \text{ при } c = 0, \dots, 2^{m-2} - 1.$$

Зафиксируем $c \in \{0, \dots, 2^{m-2} - 1\}$ и рассмотрим $W_0^{(c)} = \langle ua^c \rangle$. Тогда $\mathbf{W}^{(c)} = \{W_0^{(c)}, \dots, W_{2^{m-2}-1}^{(c)}\}$ — множество всех правых смежных классов по подгруппе $W_0^{(c)}$, где

$$W_j^{(c)} = \{a^j, ua^{j+c}, a^{2^{m-2}+j}, ua^{2^{m-2}+c+j}\} \text{ для } j = 0, \dots, 2^{m-2} - 1.$$

Ясно, что $\mathbf{U}^{(c)} = \{U_0^{(c)}, \dots, U_{2^{m-2}-1}^{(c)}\}$ — множество всех левых смежных классов, где

$$U_j^{(c)} = \{a^j, ua^{c-j}, a^{2^{m-2}+j}, ua^{2^{m-2}+c-j}\} \text{ для } j = 0, \dots, 2^{m-2} - 1.$$

Очевидно, что $\mathbf{W}^{(c)} \neq \mathbf{U}^{(c)}$. Поэтому $W_0^{(c)} \not\trianglelefteq Q_{2^m}$ для каждого $c \in \{0, \dots, 2^{m-2} - 1\}$.

Пусть H_m — модулярная максимально-циклическая группа M_{2^m} . Нетрудно убедиться, что порядок циклической группы $W_0^{(c)} = \langle ua^c \rangle$ равен $2^{m-1-\|c\|_2}$. Очевидно, что $\langle u \rangle \not\trianglelefteq M_{2^m}$ при $c = 0$.

Зафиксируем произвольное $c \in \{1, \dots, 2^{m-2} - 1\}$. Рассмотрим разбиения

$$\mathbf{W}^{(c)} = \{W_0^{(c)}, \dots, W_{2^{\|c\|_2+1}-1}^{(c)}\}, \mathbf{U}^{(c)} = \{U_0^{(c)}, \dots, U_{2^{\|c\|_2+1}-1}^{(c)}\}$$

группы M_{2^m} соответственно на правые и левые смежные классы по подгруппе $W_0^{(c)}$, где для каждого $i \in \{0, \dots, 2^{\|c\|_2+1} - 1\}$ справедливы равенства

$$W_i^{(c)} = \langle ua^c \rangle a^i = \bigcup_{j=0}^{2^{m-2}-\|c\|_2-1} \{a^{2jc+2^{m-2}jc+i}, ua^{2jc+2^{m-2}jc+c+i}\},$$

$$U_i^{(c)} = a^i \langle ua^c \rangle = \bigcup_{j=0}^{2^{m-2}-\|c\|_2-1} \{a^{2jc+2^{m-2}jc+i}, ua^{2jc+2^{m-2}jc+c+i+2^{m-2}i}\},$$

здесь использованы равенства

$$a^i(ua^c)^{2j+1} = a^i ua^{2jc+2^{m-2}jc+c} = ua^{2jc+2^{m-2}(jc+i)+c+i}$$

для $j \in \{0, \dots, 2^{m-2-\|c\|_2} - 1\}$.

Очевидно, что $W_i^{(c)} = U_i^{(c)}$ при любом четном $i \in \{0, \dots, 2^{\|c\|_2+1} - 1\}$.

Рассмотрим далее блоки $W_i^{(c)}$, $U_i^{(c)}$ для произвольного нечетного $i \in \{0, \dots, 2^{\|c\|_2+1} - 1\}$.

Пусть сначала $\|c\|_2 = m - 2$. Тогда

$$W_i^{(c)} = \{a^i, ua^{c+i}\}, U_i^{(c)} = \{a^i, ua^{c+i+2^{m-2}}\}.$$

Ясно, что $W_i^{(c)} \neq U_i^{(c)}$, а поэтому $W_0^{(c)} \not\leq M_{2m}$, если $\|c\|_2 = m - 2$.

Предположим теперь, что $\|c\|_2 \leq m - 3$. Положим

$$j' = j + 2^{m-3-\|c\|_2} \bmod 2^{m-1},$$

где $j \in \{0, \dots, 2^{m-2-\|c\|_2} - 1\}$. Так как

$$2j'c + 2^{m-2}j'c + c + i \equiv 2jc + 2^{m-2}jc + c + i + 2^{m-2}i \pmod{2^{m-1}},$$

то $W_i^{(c)} = U_i^{(c)}$ при каждом нечетном $i \in \{0, \dots, 2^{\|c\|_2+1} - 1\}$. Значит, $\mathbf{W}^{(c)} = \mathbf{U}^{(c)}$. Следовательно, $W_0^{(c)} \triangleleft M_{2m}$ при $0 < \|c\|_2 \leq m - 3$.

Пусть H_m — полудиэдральная группа SD_{2^m} . Зафиксируем произвольное $c \in \{1, \dots, 2^{m-1} - 1\}$. Нетрудно проверить, что

$$|\langle ua^c \rangle| = \begin{cases} 4, & \text{если } c \equiv 1 \pmod{2}, \\ 2, & \text{если } c \equiv 0 \pmod{2}. \end{cases}$$

Рассмотрим разбиения $\mathbf{W}^{(c)}$, $\mathbf{U}^{(c)}$ группы SD_{2^m} соответственно на правые и левые смежные классы по подгруппе $W_0^{(c)} = \langle ua^c \rangle$. Заметим, что

$$a^i ua^c = ua^{c-i+2^{m-2}} \text{ для } i = 0, \dots, 2^{m-2} - 1.$$

Зафиксируем произвольное четное $c \in \{0, 1, \dots, 2^{m-1} - 1\}$. Тогда

$$W_i^{(c)} = \{a^i, ua^{c+i}\}, U_i^{(c)} = \{a^i, ua^{c-i+2^{m-2}}\},$$

где $W_i^{(c)}$ — правый смежный класс, $U_i^{(c)}$ — левый смежный класс, $i \in \{0, \dots, 2^{m-2} - 1\}$. Отсюда следует, что $\mathbf{W}^{(c)} \neq \mathbf{U}^{(c)}$ и $W_0^{(c)} \not\leq \text{SD}_{2^m}$ для четного c .

Зафиксируем теперь произвольное нечетное число $c \in \{1, \dots, 2^{m-1} - 1\}$. Тогда

$$W_i^{(c)} = \left\{ a^i, ua^{c+i}, a^{2^{m-2}+i}, ua^{2^{m-2}+c+i} \right\},$$

$$U_i^{(c)} = \left\{ a^i, ua^{c-i+2^{m-2}}, a^{2^{m-2}+i}, ua^{c-i} \right\},$$

где $W_i^{(c)}$ — правый смежный класс, $U_i^{(c)}$ — левый смежный класс, $i \in \{0, \dots, 2^{m-3} - 1\}$. Значит, $\mathbf{W}^{(c)} \neq \mathbf{U}^{(c)}$ и $W_0^{(c)} \not\leq \text{SD}_{2^m}$ для нечетного c .

Таким образом, $\langle ua^c \rangle \not\leq \text{SD}_{2^m}$ для каждого $c \in \{0, 1, \dots, 2^{m-1} - 1\}$. $\square$

Для всех неабелевых групп H_m порядка 2^m , обладающих циклической подгруппой индекса два, приведем пример $\otimes_{\mathbf{W}}$ -марковских подстановок из $S(X)$ для разбиения $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$, блоками которого являются все правые смежные классы по подгруппе $(W_0, \otimes)$, причем $W_0 \not\leq H_m$.

Теорема 2. Пусть $m \geq 4$, $H_m \in \{D_{2^m}, Q_{2^m}, M_{2^m}, \text{SD}_{2^m}\}$, $H_m = \langle u, a \rangle$, $c \in C(H_m)$, $\mathbf{W}^{(c)}$ — множество всех правых смежных классов группы H_m по подгруппе $\langle ua^c \rangle$. Тогда подстановка

$$b^{(c)} = \prod_{j=0}^{2^{m-1}-1} (a^j, ua^{j+c}) \quad (7)$$

является $\cdot_{\mathbf{W}^{(c)}}$ -марковской. Кроме того, $b^{(c)}$ — $\cdot_{\mathbf{U}^{(c)}}$ -марковская подстановка для каждого укрупнения $\mathbf{U}^{(c)}$ разбиения $\mathbf{W}^{(c)}$, удовлетворяющего условиям леммы 1.

Доказательство. Для каждой из групп D_{2^m} , Q_{2^m} , M_{2^m} , SD_{2^m} покажем, что $\hat{\mathbf{p}}_{\mathbf{W}^{(c)}}(b^{(c)}) = \left(\hat{p}_{W_j^{(c)}, W_i^{(c)}}(b^{(c)}) \right)$ — подстановочная матрица.

Рассмотрим группу диэдра D_{2^m} . Зафиксируем произвольное $j \in \{0, \dots, 2^{m-1} - 1\}$. Из доказательства леммы 2 следует, что $W_j^{(c)} = \{a^j, ua^{j+c}\}$ — j -й правый смежный класс группы D_{2^m} по подгруппе $\langle ua^c \rangle$. Нетрудно убедиться, что для каждых $i, t \in \{0, \dots, 2^{m-1} - 1\}$ справедливы равенства

$$W_t^{(c)} \cdot (a^i)^{b^{(c)}} = \{a^t, ua^{t+c}\} \cdot ua^{i+c} = \{ua^{i+c-t}, a^{i-t}\} = W_{i-t}^{(c)},$$

$$W_t^{(c)} \cdot (ua^i)^{b(c)} = \{a^t, ua^{t+c}\} \cdot a^{i-c} = \{a^{i+t-c}, ua^{i+t}\} = W_{i+t-c}^{(c)}.$$

Отсюда для каждого $j \in \{0, \dots, 2^{m-1} - 1\}$ вытекают равенства

$$\hat{p}_{a^j, W_{2^{m-1}-j}^{(c)}}(b^{(c)}) = \hat{p}_{ua^{j+c}, W_{2^{m-1}-j}^{(c)}}(b^{(c)}) = 1.$$

Таким образом, $\hat{\mathbf{p}}_{\mathbf{W}^{(c)}}(b^{(c)}) = \left(\hat{p}_{W_j^{(c)}, W_i^{(c)}}(b^{(c)}) \right)$ — подстановочная матрица, причем

$$\hat{p}_{W_j^{(c)}, W_i^{(c)}}(b^{(c)}) = \begin{cases} 1, & \text{если } i \equiv 2^{m-1} - j \pmod{2^{m-1}}, \\ 0, & \text{если } i \not\equiv 2^{m-1} - j \pmod{2^{m-1}}. \end{cases}$$

Рассмотрим обобщенную группу кватернионов Q_{2^m} . Положим

$$W_t^{(0,c)} = \{a^t, a^{2^{m-2}+t}\}, \quad W_t^{(1,c)} = \{ua^{t+c}, ua^{2^{m-2}+c+t}\},$$

$$W_t^{(c)} = W_t^{(0,c)} \cup W_t^{(1,c)} \text{ для } t = 0, \dots, 2^{m-2} - 1.$$

Зафиксируем произвольное число $j \in \{0, \dots, 2^{m-2} - 1\}$. Из доказательства леммы 2 следует, что $W_j^{(c)}$ — j -й правый смежный класс группы Q_{2^m} по подгруппе $\langle ua^c \rangle$, где $j \in \{0, \dots, 2^{m-2} - 1\}$.

Для любых $i, t \in \{0, \dots, 2^{m-1} - 1\}$ справедливы цепочки равенств:

$$W_t^{(0,c)} \cdot (a^i)^{b(c)} = \{a^t, a^{2^{m-2}+t}\} \cdot ua^{i+c} = \{ua^{i-t+c}, ua^{2^{m-2}+i-t+c}\} = W_{i-t}^{(1,c)},$$

$$W_t^{(1,c)} \cdot (a^i)^{b(c)} = \{ua^{t+c}, ua^{2^{m-2}+c+t}\} \cdot ua^{i+c} = \{a^{2^{m-2}+i-t}, a^{i-t}\} = W_{i-t}^{(0,c)},$$

$$W_t^{(0,c)} \cdot (ua^i)^{b(c)} = \{a^t, a^{2^{m-2}+t}\} \cdot a^{i-c} = \{a^{i+t-c}, a^{2^{m-2}+i+t-c}\} = W_{i+t-c}^{(0,c)},$$

$$W_t^{(1,c)} \cdot (ua^i)^{b(c)} = \{ua^{t+c}, ua^{2^{m-2}+c+t}\} \cdot a^{i-c} = \{ua^{i+t}, ua^{2^{m-2}+i+t}\} = W_{i+t-c}^{(1,c)}.$$

Отсюда следует, что для каждого $j \in \{0, \dots, 2^{m-2} - 1\}$ выполняются равенства

$$\hat{p}_{a^j, W_{2^{m-2}-j}^{(0,c)}}(b^{(c)}) = \hat{p}_{a^{2^{m-2}+j}, W_{2^{m-2}-j}^{(0,c)}}(b^{(c)}) = 1,$$

$$\hat{p}_{ua^{j+c}, W_{2^{m-2}-j}^{(1,c)}}(b^{(c)}) = \hat{p}_{ua^{2^{m-2}+j+c}, W_{2^{m-2}-j}^{(1,c)}}(b^{(c)}) = 1.$$

Таким образом, $\hat{\mathbf{p}}_{\mathbf{W}^{(c)}}(b^{(c)}) = \left(\hat{p}_{W_j^{(c)}, W_i^{(c)}}(b^{(c)}) \right)$ — подстановочная матрица.

Рассмотрим группу $M_{2^m} = \langle u, a \rangle$. Зафиксируем произвольное $j \in \{0, \dots, 2^{m-2} - 1\}$.

Из доказательства леммы 2 следует, что $W_j^{(c)}$ — j -й правый смежный класс группы M_{2^m} по подгруппе $\langle ua^c \rangle$, где $j \in \{0, \dots, 2^{m-2} - 1\}$. Для любых $i, t \in \{0, \dots, 2^{m-1} - 1\}$ справедливы цепочки равенств

$$\begin{aligned} W_t^{(c)} \cdot (a^i)^{b^{(c)}} &= \{a^t, ua^{t+c}\} \cdot ua^{i+c} = \{a^t ua^{i+c}, ua^{t+c} ua^{i+c}\} \\ &= \left\{ ua^{i+c+t+t2^{m-2}}, a^{i+c+t+c+(t+c)2^{m-2}} \right\} \\ &= \left\{ ua^{i+c+t+t2^{m-2}}, a^{i+t+t2^{m-2}} \right\} = W_{i+t+t2^{m-2}}^{(c)}, \\ W_t^{(c)} \cdot (ua^i)^{b^{(c)}} &= \{a^t, ua^{t+c}\} \cdot a^{i-c} = \{a^t a^{i-c}, ua^{t+c} a^{i-c}\} \\ &= \{a^{t+i-c}, ua^{t+i}\} = W_{i+t-c}^{(c)}. \end{aligned}$$

Отсюда следует, что для каждого $j \in \{0, \dots, 2^{m-1} - 1\}$ справедливы равенства

$$\hat{p}_{a^j, W_j^{(c)}}_{j(2^{m-2}+1) \bmod 2^{m-1}}(b^{(c)}) = \hat{p}_{ua^{j+c}, W_{j(2^{m-2}+1) \bmod 2^{m-1}}^{(c)}}(b^{(c)}) = 1.$$

Таким образом, $\hat{\mathbf{p}}_{\mathbf{W}^{(c)}}(b^{(c)}) = \left(\hat{p}_{W_j^{(c)}, W_i^{(c)}}(b^{(c)}) \right)$ — подстановочная матрица, причем

$$\hat{p}_{W_j^{(c)}, W_i^{(c)}}(b^{(c)}) = \begin{cases} 1, & \text{если } i \equiv j(2^{m-2} + 1) \pmod{2^{m-1}}, \\ 0, & \text{если } i \not\equiv j(2^{m-2} + 1) \pmod{2^{m-1}}. \end{cases}$$

Рассмотрим группу $\text{SD}_{2^m} = \langle u, a \rangle$. Положим

$$T_i^{(c)} = \{a^i, ua^{i+c}\} \text{ для } i = 0, \dots, 2^{m-1} - 1.$$

Из доказательства леммы 2 следует, что блоки разбиения $\mathbf{W}^{(c)} = \{W_0^{(c)}, \dots, W_{r_c-1}^{(c)}\}$ суть

$$W_i^{(c)} = \begin{cases} T_i^{(c)}, & \text{если } c \equiv 0 \pmod{2}, \\ T_i^{(c)} \cup T_{i+2^{m-2}}^{(c)}, & \text{если } c \equiv 1 \pmod{2}, \end{cases}$$

где

$$r_c = \begin{cases} 2^{m-1}, & \text{если } c \equiv 0 \pmod{2}, \\ 2^{m-2}, & \text{если } c \equiv 1 \pmod{2}. \end{cases}$$

Зафиксируем произвольное $j \in \{0, \dots, 2^{m-1} - 1\}$. Для любых $i, t \in \{0, \dots, 2^{m-1} - 1\}$ справедливы цепочки равенств

$$\begin{aligned} T_t^{(c)} \cdot (ua^i)^{b^{(c)}} &= \{a^t, ua^{t+c}\} \cdot a^{i-c} = \{a^t a^{i-c}, ua^{t+c} a^{i-c}\} \\ &= \{a^{t+i-c}, ua^{t+i}\} = T_{i+t-c}^{(c)}, \end{aligned} \quad (8)$$

$$\begin{aligned} T_t^{(c)} \cdot (a^i)^{b^{(c)}} &= \{a^t, ua^{t+c}\} \cdot ua^{i+c} \\ &= \{a^t ua^{i+c}, ua^{t+c} ua^{i+c}\} = \left\{ ua^{i-t+c+t2^{m-2}}, a^{i-t+t2^{m-2}+2^{m-2}c} \right\}. \end{aligned} \quad (9)$$

Из равенств (8), (9) получаем

$$T_t^{(c)} \cdot (a^i)^{b^{(c)}} = T_{i-t+t2^{m-2}}^{(c)}, \text{ если } c \equiv 0 \pmod{2}, \quad (10)$$

$$\left(T_t^{(c)} \cup T_{t+2^{m-2}}^{(c)} \right) \cdot (a^i)^{b^{(c)}} = T_{i-t+t2^{m-2}}^{(c)} \cup T_{i-t+t2^{m-2}+2^{m-2}}^{(c)}, \quad (11)$$

если $c \equiv 1 \pmod{2}$.

Пусть $c \equiv 0 \pmod{2}$. Тогда из (8), (9) следует цепочка равенств

$$\hat{p}_{a^j, T_{j(2^{m-2}-1)}^{(c)}}(b^{(c)}) = \hat{p}_{ua^{j+c}, T_{j(2^{m-2}-1)}^{(c)}}(b^{(c)}) = 1,$$

из которых вытекает $\cdot \mathbf{W}^{(c)}$ -марковость подстановки $b^{(c)}$.

Пусть $c \equiv 1 \pmod{2}$. Тогда из (8), (11) вытекает цепочка равенств

$$\begin{aligned} \hat{p}_{a^j, W_{2^{m-2}-j}^{(c)}}(b^{(c)}) &= \hat{p}_{ua^{j+c}, W_{2^{m-2}-j}^{(c)}}(b^{(c)}) \\ &= \hat{p}_{a^{j+2^{m-2}}, W_{2^{m-2}-j}^{(c)}}(b^{(c)}) = \hat{p}_{ua^{j+c+2^{m-2}}, W_{2^{m-2}-j}^{(c)}}(b^{(c)}) = 1. \end{aligned}$$

Таким образом, для каждой из групп D_{2^m} , Q_{2^m} , M_{2^m} , SD_{2^m} доказано, что $\hat{\mathbf{P}}_{\mathbf{W}^{(c)}}(b^{(c)}) = \left(\hat{p}_{W_j^{(c)}, W_i^{(c)}}(b^{(c)}) \right)$ — подстановочная матрица. Тогда из утверждения 3 [2] и леммы 2 вытекает $\cdot \mathbf{W}^{(c)}$ -марковость подстановки $b^{(c)}$, а также ее $\cdot \mathbf{U}^{(c)}$ -марковость для каждого укрупнения $\mathbf{U}^{(c)}$ разбиения $\mathbf{W}^{(c)}$, удовлетворяющего лемме 1. $\square$

В теореме 2 приведен пример множества подстановок $\{b^{(c)} | c \in C(H_m)\}$, заданных условием (7) и являющихся $\cdot \mathbf{W}^{(c)}$ -марковскими для всех неабелевых групп порядка 2^m , обладающих циклической подгруппой индекса два. Очевидно, что такие подстановки являются криптографически «слабыми». Однако цель состояла именно в установлении существования множества $\cdot \mathbf{W}^{(c)}$ -марковских подстановок, являющихся такими для каждой из групп D_{2^m} , Q_{2^m} , M_{2^m} , SD_{2^m} , а не в построении криптографически «хорошего» класса.

5. Неабелевы группы, обладающие циклической подгруппой индекса два, и подстановочные гомоморфизмы алгоритма $C_l(\otimes, b)$

Пусть $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$, $e_X \in W_0$, W_j — j -й правый смежный класс группы $(X, \otimes)$ по подгруппе $(W_0, \otimes)$. Если группа $G = \langle b, X^\otimes \rangle$ импримитивна с системой импримитивности $\mathbf{W}$, то существует естественный гомоморфизм $\varphi_{\mathbf{W}}^{(G)} : G \rightarrow S(\{0, \dots, r-1\})$, $e_S = \varphi_{\mathbf{W}}^{(G)}(\sigma_0)$, где e_S — нейтральный элемент (тождественная подстановка). Очевидно, что если $(W_0, \otimes) \not\trianglelefteq (X, \otimes)$, то $\text{Ker} \varphi_{\mathbf{W}}^{(X^\otimes)} = \{\sigma_0\}$ тогда и только тогда, когда группа $(W_0, \otimes)$ не содержит нетривиальных нормальных подгрупп группы $(X, \otimes)$. Так как $(W_0^{(c)}, \otimes) \not\trianglelefteq (X, \otimes)$, то согласно [10] бинарную операцию $\odot$ невозможно корректно задать условием (2). Следовательно, равенство (3) не выполняется. Поэтому отображение $\varphi_{\mathbf{W}^{(c)}}^{(G)}$ не задает гомоморфизм $C_l(\otimes, b)$ в $C_l(\odot, \bar{b})$.

Далее понадобится следующий результат.

Лемма 4. Пусть:

- 1) $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$, где W_j — j -й правый смежный класс группы $(X, \otimes)$ по подгруппе $(W_0, \otimes)$, $j = 0, \dots, r-1$.
- 2) $G = \langle b, X^\otimes \rangle$, $e_X \in W_0$, $\varphi_{\mathbf{W}}^{(G)} : G \rightarrow S(\{0, \dots, r-1\})$ — естественный гомоморфизм группы G с системой импримитивности $\mathbf{W}$, причем $e_S = \varphi_{\mathbf{W}}^{(G)}(\sigma_0)$.
- 3) Существует такая максимальная подгруппа $(U_0, \otimes)$ группы $(W_0, \otimes)$, что $U_0 \triangleleft X$.

Тогда:

- 1) $|\text{Im} \varphi_{\mathbf{W}}^{(X^\otimes)}| = |X : U_0|$, $\text{Ker} \varphi_{\mathbf{W}}^{(X^\otimes)} = \rho(U_0)$.
- 2) Если $U_0 = \{e_X\}$, то $\text{Ker} \varphi_{\mathbf{W}}^{(X^\otimes)} = \{\sigma_0\}$ и $\text{Im} \varphi_{\mathbf{W}}^{(X^\otimes)} \cong X^\otimes$.
- 3) Если $\varphi_{\mathbf{W}}^{(G)}(b) = \{e_S\}$, то $|\text{Im} \varphi_{\mathbf{W}}^{(G)}| = |X : U_0|$, $\text{Ker} \varphi_{\mathbf{W}}^{(G)} = \langle \rho(U_0), b \rangle$.
- 4) $\text{Ker} \varphi_{\mathbf{W}}^{(G)} = \rho(U_0)$, если $\varphi_{\mathbf{W}}^{(G)}(b) \neq e_S$.

Доказательство. Пусть $\mathbf{U} = \{U_0, \dots, U_{q-1}\} = X : U_0$. По условию

$$U_0 \trianglelefteq X, U_0 \leq W_0, r \leq q \leq |X|.$$

Тогда

$$U_i = U_0 \otimes \delta_i = \delta_i \otimes U_0$$

для произвольного фиксированного элемента $\delta_i \in U_i$, $i = 0, \dots, q-1$.

Очевидно, что из условия $U_i \cap W_0 \neq \emptyset$ для некоторого $i \in \{0, \dots, q-1\}$ вытекает включение $U_i \subseteq W_0$. Следовательно, существует такое $J_0 \subseteq \{0, \dots, q-1\}$, что $W_0 = \bigcup_{t \in J_0} U_t$. Так как $W_i = W_0 \otimes \theta_i$ для произвольного фиксированного элемента $\theta_i \in W_i$, то

$$W_i = \bigcup_{t \in J_0} (U_t \otimes \theta_i) = \bigcup_{t \in J_0} (U_0 \otimes \delta_t \otimes \theta_i) \text{ для } i = 0, \dots, r-1.$$

Поэтому существует такое разбиение $\mathbf{J} = \{J_0, \dots, J_{r-1}\}$ множества $\{0, \dots, q-1\}$, что $W_i = \bigcup_{t \in J_i} U_t$ для $i = 0, \dots, r-1$.

П.1. Очевидно, что

$$\text{Ker} \varphi_{\mathbf{W}}^{(X^\otimes)} = \{\sigma_k \in X^\otimes \mid W_i \otimes k = W_i \ \forall i \in \{0, \dots, r-1\}\},$$

$$\text{Ker} \varphi_{\mathbf{W}}^{(X^\otimes)} \leq \rho(W_0).$$

Так как

$$\text{Ker} \varphi_{\mathbf{W}}^{(X^\otimes)} \trianglelefteq X^\otimes, \ U_0 \leq W_0, \ \rho(U_0) \trianglelefteq X^\otimes,$$

$$W_i \otimes k = W_i \text{ для всех } k \in U_0, i \in \{0, \dots, r-1\},$$

то из условий нормальности и максимальности подгруппы U_0 в W_0 вытекает равенство $\text{Ker} \varphi_{\mathbf{W}}^{(X^\otimes)} = \rho(U_0)$. Отсюда следует, что

$$\left| \text{Im} \varphi_{\mathbf{W}}^{(X^\otimes)} \right| = |X^\otimes : \rho(U_0)| = |X : U_0|.$$

Пп. 2, 3, 4. Из п.1 следует, что если $U_0 = \{e_X\}$, то

$$\text{Ker} \varphi_{\mathbf{W}}^{(X^\otimes)} = \{\sigma_0\}, \ \text{Im} \varphi_{\mathbf{W}}^{(X^\otimes)} \cong X^\otimes.$$

Из п.1 также вытекает, что если $\varphi_{\mathbf{W}}^{(G)}(b) = e_S$, то

$$\text{Ker} \varphi_{\mathbf{W}}^{(G)} = \langle \rho(U_0), b \rangle, \ \left| \text{Im} \varphi_{\mathbf{W}}^{(G)} \right| = \left| \text{Im} \varphi_{\mathbf{W}}^{(X^\otimes)} \right| = |X : U_0|.$$

Очевидно, что если $\varphi_{\mathbf{W}}^{(G)}(b) \neq e_S$, то $\text{Ker} \varphi_{\mathbf{W}}^{(G)} = \rho(U_0)$. □

Далее $\mathbb{Z}_{2^n}^+$ — группа сдвигов аддитивной группы кольца вычетов $\mathbb{Z}_{2^n}$.

5.1. Гомоморфизмы алгоритма $C_l(\otimes, b)$ и диэдральная группа

Рассмотрим группу диэдра D_{2^m} порядка 2^m , $m \geq 3$, $(X, \otimes) = (D_{2^m}, \cdot)$.

Пусть c — произвольный элемент множества $\{0, \dots, 2^{m-1} - 1\}$, $\mathbf{W}^{(c)} = \{W_0^{(c)}, \dots, W_{2^{m-1}-1}^{(c)}\}$ — множество всех правых смежных классов группы D_{2^m} по подгруппе $\langle ua^c \rangle$, где

$$W_j^{(c)} = \{a^j, ua^{j+c}\} \text{ для } j = 0, \dots, 2^{m-1} - 1.$$

Положим $\mathbf{W} = \mathbf{W}^{(0)}$. Нетрудно убедиться в том, что для каждого $x \in D_{2^m}$ подстановка $\varphi_{\mathbf{W}}^{(X^\otimes)}(x) : \{0, \dots, 2^{m-1} - 1\} \rightarrow \{0, \dots, 2^{m-1} - 1\}$ задана условием

$$\begin{aligned} & \varphi_{\mathbf{W}}^{(X^\otimes)}(x) : i \\ \mapsto & \begin{cases} i + j \pmod{2^{m-1}}, & \text{если } x = a^j, j \in \{0, \dots, 2^{m-1} - 1\}, \\ 2^{m-1} - i \pmod{2^{m-1}}, & \text{если } x = u, \\ 2^{m-1} - i + j \pmod{2^{m-1}}, & \text{если } x = ua^j, j \in \{0, \dots, 2^{m-1} - 1\}, \end{cases} \end{aligned}$$

для каждого $i \in \{0, \dots, 2^{m-1} - 1\}$.

Очевидно, что у группы $W_0^{(0)} = \{e, u\}$ нет нетривиальных нормальных подгрупп. Согласно пп. 2, 3 леммы 4 справедливы равенства

$$\text{Ker} \varphi_{\mathbf{W}}^{(X^\otimes)} = \{\sigma_0\}, \quad \text{Im} \varphi_{\mathbf{W}}^{(X^\otimes)} \cong \left\langle \mathbb{Z}_{2^{m-1}}^+, \prod_{i=0}^{2^{m-2}-1} (i, 2^{m-1} - i) \right\rangle \cong D_{2^m}.$$

Если $\varphi_{\mathbf{W}}^{(G)}(b) \neq e_S$, то $\text{Ker} \varphi_{\mathbf{W}}^{(G)} = \{\sigma_0\}$, где $G = \langle b, X^\otimes \rangle$. Следовательно, отображение $\varphi_{\mathbf{W}}^{(G)}$ — изоморфизм, а группа G изоморфна подгруппе

$$\varphi_{\mathbf{W}}^{(G)}(G) = \left\langle \mathbb{Z}_{2^{m-1}}^+, \varphi_{\mathbf{W}}^{(G)}(b), \prod_{i=0}^{2^{m-2}-1} (i, 2^{m-1} - i) \right\rangle$$

группы $S(\{0, \dots, 2^{m-1} - 1\})$.

Заметим, что группа $\mathbb{Z}_{2^{m-1}}^+$ импримитивна с системами импримитивности $\widetilde{\mathbf{W}}^{(t)} = \{\widetilde{W}_0^{(t)}, \dots, \widetilde{W}_{2^{m-1}-t-1}^{(t)}\}$ при $t = 1, \dots, m-2$, где

$$\widetilde{W}_j^{(t)} = \{\alpha \in \mathbb{Z}_{2^{m-1}} \mid \alpha \equiv j \pmod{2^{m-1-t}}\}$$

для $j = 0, \dots, 2^{m-1-t} - 1$.

Очевидно, что подстановка $\prod_{i=0}^{2^{m-2}-1} (i, 2^{m-1} - i)$ сохраняет систему импримитивности $\widetilde{\mathbf{W}}^{(t)}$. Таким образом, число систем импримитивности группы $\text{Im}\varphi_{\mathbf{W}}^{(X^{\otimes})}$ порядка 2^m равно $m - 2$.

Если подстановка b такова, что $\varphi_{\mathbf{W}}^{(G)}(b)$ не сохраняет систему импримитивности $\widetilde{\mathbf{W}}^{(t)}$ для каждого $t \in \{1, \dots, m-2\}$, то группа $\varphi_{\mathbf{W}}^{(G)}(G)$ примитивна. Согласно [8] группа $\varphi_{\mathbf{W}}^{(G)}(G)$ изоморфна $S_{2^{m-1}}$ или подстановочно изоморфна естественному подстановочному представлению степени 2^{m-1} проективной линейной группы $PGL_2(2^{m-1} - 1)$, если $2^{m-1} - 1$ — простое число.

Алгоритмы $C_l(\otimes, b)$ с подстановками b , а также разбиениями $\mathbf{W}^{(c)}$, описанными в теореме 2, являются примерами $\otimes_{\mathbf{W}}$ -марковских алгоритмов, для которых отображение $\varphi_{\mathbf{W}^{(c)}}^{(G)}$ определяет (изоморфное) вложение группы $G = \langle b, X^{\otimes} \rangle$ в $S_{2^{m-1}}$. Так как $(W_0^{(c)}, \otimes) \not\leq (X, \otimes)$, то согласно [10] бинарную операцию $\odot$ невозможно корректно задать условием (2). Следовательно, равенство (3) не выполняется. Поэтому отображение $\varphi_{\mathbf{W}^{(c)}}^{(G)}$ не задает гомоморфизм $C_l(\otimes, b)$ в $C_l(\odot, \bar{b})$.

Рассмотрим подгруппы группы диэдра D_{2^m} , порядок которых больше двух. Нетрудно убедиться, что любая такая подгруппа порядка 2^t имеет вид $G^{(q_t)} = \langle u, a^{q_t} \rangle$, где $q_t \equiv 0 \pmod{2^{m-t}}$ и $q_t \not\equiv 0 \pmod{2^{m-t-1}}$.

Очевидно, что так как $G^{(q_t)} = \langle a^{q_t} \rangle \cup u \langle a^{q_t} \rangle$, то $G^{(q_t)} \triangleleft D_{2^m}$. Отсюда следует, что $B \not\leq D_{2^m}$ тогда и только тогда, когда $B \in \{\langle ua^c \rangle \mid c = 0, \dots, 2^{m-2} - 1\}$.

Из теоремы 1 вытекает, что если $\mathbf{W}^{(q_t)}$ — множество всех смежных классов группы D_{2^m} по подгруппе $G^{(q_t)}$, то отображение $\varphi_{\mathbf{W}^{(q_t)}}^{(G)}$ задает гомоморфизм $C_l(\otimes, b)$ в $C_l(\odot, \bar{b})$.

5.2. Гомоморфизмы алгоритма $C_l(\otimes, b)$ и обобщенная кватернионная группа

Рассмотрим обобщенную группу кватернионов Q_{2^m} порядка 2^m , $m \geq 4$, $(X, \otimes) = (Q_{2^m}, \cdot)$, а также ее подгруппы порядка четыре

$$W_0^{(c)} = \langle ua^c \rangle = \left\{ e, ua^c, a^{2^{m-2}}, ua^{2^{m-2}+c} \right\} \text{ при } c = 0, \dots, 2^{m-2} - 1.$$

Зафиксируем $c \in \{0, \dots, 2^{m-2} - 1\}$ и рассмотрим $W_0^{(c)} = \langle ua^c \rangle$. Очевидно, что $W_0^{(c)} \not\leq Q_{2^m}$, а $\mathbf{W}^{(c)} = \{W_0^{(c)}, \dots, W_{2^{m-2}-1}^{(c)}\}$ — множество

всех правых смежных классов по подгруппе $W_0^{(c)}$, где

$$W_j^{(c)} = \{a^j, ua^{j+c}, a^{2^{m-2}+j}, ua^{2^{m-2}+c+j}\} \text{ для } j = 0, \dots, 2^{m-2} - 1.$$

Положим $\mathbf{W} = \mathbf{W}^{(0)}$. Нетрудно убедиться в том, что для каждого $x \in Q_{2^m}$ подстановка $\varphi_{\mathbf{W}}^{(X^{\otimes})}(x) : \{0, \dots, 2^{m-2} - 1\} \rightarrow \{0, \dots, 2^{m-2} - 1\}$ задана условием

$$\begin{aligned} & \varphi_{\mathbf{W}}^{(X^{\otimes})}(x) : i \mapsto \\ & \mapsto \begin{cases} i + j \pmod{2^{m-2}}, & \text{если } x = a^j, j \in \{0, \dots, 2^{m-2} - 1\}, \\ 2^{m-2} - i \pmod{2^{m-2}}, & \text{если } x = u, \\ 2^{m-2} - i + j \pmod{2^{m-2}}, & \text{если } x = ua^j, j \in \{0, \dots, 2^{m-2} - 1\}, \end{cases} \end{aligned}$$

для каждого $i \in \{0, \dots, 2^{m-1} - 1\}$.

Очевидно, что у группы $W_0^{(0)} = \langle u \rangle$, Q_{2^m} есть нетривиальная нормальная подгруппа $\langle a^{2^{m-2}} \rangle$ порядка два.

Согласно п. 2 леммы 4 справедливы равенства

$$\begin{aligned} \text{Ker} \varphi_{\mathbf{W}}^{(X^{\otimes})} & \cong \langle a^{2^{m-2}} \rangle, \\ \text{Im} \varphi_{\mathbf{W}}^{(X^{\otimes})} & \cong \left\langle \mathbb{Z}_{2^{m-2}}^+, \prod_{i=0}^{2^{m-3}-1} (i, 2^{m-2} - i) \right\rangle \cong D_{2^{m-1}}. \end{aligned}$$

Рассмотрим подгруппы обобщенной группы кватернионов Q_{2^m} , порядок которых больше четырех. Нетрудно убедиться, что любая такая подгруппа порядка 2^{t+1} имеет вид $G^{(q_t)} = \langle u, a^{q_t} \rangle$, где

$$q_t \equiv 2^{m-t-2} \pmod{2^{m-t-1}} \text{ для } t = 1, \dots, m-2.$$

Так как $G^{(q_t)} = \langle a^{q_t} \rangle \cup u \langle a^{q_t} \rangle$, то $G^{(q_t)} \triangleleft Q_{2^m}$. Отсюда следует, что $B \not\leq Q_{2^m}$ тогда и только тогда, когда $B \in \{\langle ua^c \rangle \mid c = 0, \dots, 2^{m-2} - 1\}$.

Из теоремы 1 вытекает, что если $\mathbf{W}^{(q_t)}$ — разбиение Q_{2^m} на смежные классы по подгруппе $G^{(q_t)}$, то отображение $\varphi_{\mathbf{W}^{(q_t)}}^{(X^{\otimes})}$ задает гомоморфизм $C_l(\otimes, b)$ в $C_l(\odot, \bar{b})$.

Список литературы

- [1] Lai X., Massey J. L., Murphy S., “Markov ciphers and differential cryptanalysis”, EUROCRYPT 1991, Lect. Notes Comput. Sci., **547**, 1991, 17–38.
- [2] Погорелов Б. А., Пудовкина М. А., “Разбиения на биграммах и марковость алгоритмов блочного шифрования”, *Математические вопросы криптографии*, **8**:1 (2017), 5–40.
- [3] Погорелов Б. А., Пудовкина М. А., “Подстановочные гомоморфизмы алгоритмов блочного шифрования и $\otimes \mathbf{w}$ -марковость”, *Математические вопросы криптографии*, **9**:3 (2018), 109–126.
- [4] Кемени Д., Снелл Д., *Конечные цепи Маркова*, М.: Наука, 1970, 272 с.
- [5] Холл М., *Теория групп*, М.: ИЛ, 1962, 468 с.
- [6] Humphreys J. F., *A course in group theory*, Oxford Univ. Press, 1996, 279 с.
- [7] Погорелов Б. А., Пудовкина М. А., “ $\otimes \mathbf{w}$ -марковость XSL-алгоритмов блочного шифрования, связанная со свойствами слоев раундовой функции”, *Математические вопросы криптографии*, **10**:1 (2019), 115–143.
- [8] Погорелов Б. А., “Примитивные группы подстановок, содержащие 2^m -цикл”, *Алгебра и логика*, **19**:2 (1980), 236–247.
- [9] Сачков В. Н., *Введение в комбинаторные методы дискретной математики*, 2-е изд., М.: МЦНМО, 2004, 424 с.
- [10] Винберг Э. Б., *Курс алгебры*, 2-е изд., испр. и доп., М.: Факториал Пресс, 2001, 544 с.
- [11] Глухов М. М., Елизаров В. П., Нечаев А. А., *Алгебра*, 2-е изд., испр. и доп., СПб.: Лань, 2015, 608 с.