

Подстановочные гомоморфизмы алгоритмов блочного шифрования и $\otimes_{\mathbf{W}}$ -марковость

Б. А. Погорелов¹, М. А. Пудовкина²

¹ Академия криптографии Российской Федерации, Москва

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

Получено 11.V.2017

Аннотация. Известно (Lai X., Massey J. L., Murphy S., 1991), что последовательность раундовых разностей в \otimes -марковских алгоритмах блочного шифрования с независимыми равномерно распределенными раундовыми ключами, алфавитом текстов X , абелевой группой (X, \otimes) наложения ключа является марковской цепью. В 2017 году авторы указали условия, при которых укрупнение разностей (описываемое разбиением \mathbf{W}) \otimes -марковского алгоритма дает снова марковскую цепь. Алгоритмы с таким свойством названы $\otimes_{\mathbf{W}}$ -марковскими. Здесь продолжается исследование свойств $\otimes_{\mathbf{W}}$ -марковских алгоритмов. Выясняется связь между существованием гомоморфизмов у алгоритмов блочного шифрования и $\otimes_{\mathbf{W}}$ -марковостью.

Ключевые слова: марковский алгоритм блочного шифрования, цепь Маркова, укрупнение состояний, $\otimes_{\mathbf{W}}$ -марковость, подстановочный гомоморфизм

Permutation homomorphisms of block ciphers and $\otimes_{\mathbb{W}}$ -Markovian property

B. A. Pogorelov¹, **M. A. Pudovkina**²

¹ *Academy of Cryptography of the Russian Federation, Moscow*

² *Bauman Moscow State Technical University, Moscow*

Abstract. We consider \otimes -Markov block ciphers on the alphabet X with independent round keys and an Abelian group (X, \otimes) of key addition. Lai X., Massey J. L., Murphy S. in 1991 had proved that the sequence of round differences of the \otimes -Markov block cipher forms a Markov chain. In 2017 we have given conditions under which the sequence of lumped round differences of the \otimes -Markov block cipher is again a Markov chain. Ciphers with such property were called $\otimes_{\mathbb{W}}$ -Markovian block ciphers. The definition of $\otimes_{\mathbb{W}}$ -Markovian block ciphers naturally leads to a notion of $\otimes_{\mathbb{W}}$ -Markovian transformations. In this paper, we continue to investigate properties of $\otimes_{\mathbb{W}}$ -Markovian ciphers. We ascertain connections between the existence of homomorphisms of block ciphers and the $\otimes_{\mathbb{W}}$ -Markovian property.

Key words: Markov block cipher, Markov chain, lumped states, $\otimes_{\mathbb{W}}$ -Markovian property, permutation homomorphism

Citation: *Mathematical Aspects of Cryptography*, 2018, v. 9, № 3, pp. 109–126 (Russian)

© Академия криптографии Российской Федерации, 2018 г.

1. Введение

Требования к алгоритмам развертывания ключа все в большей степени приближаются к требованиям, предъявляемым к качественным генераторам псевдослучайных последовательностей, например последовательность раундовых ключей должна быть неотличима (полиномиальными и вероятностными алгоритмами) от случайной идеальной последовательности. Реализация этих требований в реальных шифрсистемах является дополнительным обоснованием применимости марковской модели блочных шифрсистем в более общей ситуации, а не только в случае независимых раундовых ключей (см. [3]). В рамках марковской модели удается обосновать стойкость синтезируемых шифрсистем относительно ряда методов криптоанализа, в том числе с помощью теоретико-группового подхода [4].

Марковость алгоритмов блочного шифрования впервые была рассмотрена в [1] в связи с обоснованием стойкости относительно линейного и разностного методов криптоанализа. Свойствам цепей Маркова вероятностных преобразователей и итерационных преобразований посвящены также работы [5–9], а укрупнения цепей Маркова — [10]. Все это вместе с возрастающими требованиями к алгоритмам развертывания ключа говорит о целесообразности дальнейшего развития марковского подхода (например, рассмотрением близких к марковским моделей) при исследовании алгоритмов блочного шифрования.

Марковость алгоритмов блочного шифрования на языке теории автоматов может быть интерпретирована следующим образом. Рассматривается последовательность случайных величин, соответствующая биграммам (парам блоков) промежуточных текстов. Биграммы текстов можно считать состояниями конечного детерминированного автомата, на вход которого поступают раундовые ключи (случайно и равновероятно выбираемые из множества всех раундовых ключей K), а функция переходов задается раундовой функцией $g : X \times K \rightarrow X$, действие которой естественным образом переносится на биграммы. В рамках автоматной модели (вероятностного преобразователя) получаем цепь Маркова с множеством состояний X^2 и матрицей вероятностей переходов, элементы которой заданы условием

$$p_{(\alpha_1, \alpha_0), (\alpha'_1, \alpha'_0)}(g) = \mathbf{P} \{(\alpha_1^{g_k}, \alpha_0^{g_k}) = (\alpha'_1, \alpha'_0)\}, \quad \text{где } g_k : \alpha \mapsto g(\alpha, k),$$

а раундовый ключ k выбирается случайно и равновероятно из множества K и, естественно, независимо от биграмм $(\alpha_1, \alpha_0), (\alpha'_1, \alpha'_0) \in X^2$. В этой модели рассматриваемые в разностном методе разности биграмм интерпретируются [2] как укрупнение состояний из X^2 посредством разбиения $\mathbf{X} = \{X_\varepsilon \mid \varepsilon \in X\}$, где (X, \otimes) — абелева группа с операцией сложения \otimes ,

$$X_\varepsilon = \{(\alpha \otimes \varepsilon, \alpha) \mid \alpha \in X\} \quad \text{для } \varepsilon \in X.$$

Неявно дальнейшие укрупнения последовательности разностей биграмм для некоторого класса блоков разбиений множества X и наборов номеров таких блоков используются в методе усеченных разностей — в одном из наиболее распространенных обобщений разностного метода (см. [11–15]).

В [2] рассматривались итерационные алгоритмы блочного шифрования с независимыми и равномерно распределенными раундовыми ключами, алфавитом текстов X , абелевой группой (X, \otimes) наложения ключа и разбиением \mathbf{W} множества разностей относительно операции \otimes . Были приведены условия, при которых укрупнение разностей (описываемое разбиением \mathbf{W}) \otimes -марковского алгоритма дает марковскую последовательность. Алгоритмы с таким свойством названы $\otimes_{\mathbf{W}}$ -марковскими. Существование такого разбиения \mathbf{W} может зависеть от свойств группы, порожденной раундовой функцией g , в том числе и от свойств преобразований, составляющих функцию g . В связи с этим в [2] введено понятие $\otimes_{\mathbf{W}}$ -марковского преобразования, естественным образом следующее из определения $\otimes_{\mathbf{W}}$ -марковского алгоритма блочного шифрования. Особенность $\otimes_{\mathbf{W}}$ -марковских преобразований состоит в наличии определенной структурированности их матриц переходов разностей. Кроме того, в [2] для ряда преобразований, основанных на операциях экспоненцирования и логарифмирования в кольце вычетов \mathbb{Z}_{2^d} и в поле $GF(p)$, p — простое число, указаны разбиения \mathbf{W} множества X , при которых преобразования являются $\otimes_{\mathbf{W}}$ -марковскими.

В настоящей работе продолжается исследование свойств $\otimes_{\mathbf{W}}$ -марковских алгоритмов и преобразований. Для произвольной абелевой группы (X, \otimes) 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 $g_k: x \mapsto (x \otimes k)^b$ для всех $(x, k) \in X^2$, где $\alpha^b = \alpha b = b(\alpha)$ для всех $\alpha \in X$, а частичная l -раундовая функция зашифрования $f_{\vec{k}_l}^{(l)}: X \rightarrow X$ на ключе $\vec{k}_l = (k_1, \dots, k_l) \in X^l$ определяется как $f_{\vec{k}_l}^{(l)} = g_{k_1} \cdots g_{k_l}$.

Пусть (Y, \odot) — абелева группа, $s \in S(Y)$, $|Y| < |X|$. Отображение $\theta: X \rightarrow Y$, удовлетворяющее условию $\theta((x \otimes k)^b) = (\theta(x) \odot \theta(k))^s$ для всех $(x, k) \in X^2$, называется гомоморфизмом алгоритма $C_l(\otimes, b)$ в алгоритм $C_l(\odot, s)$ (далее гомоморфизм алгоритма $C_l(\otimes, b)$).

Мы описываем связь между существованием гомоморфизма θ и $\otimes_{\mathbf{W}}$ -марковостью алгоритма $C_l(\otimes, b)$. Показано, что наложение на множество $\{g_k \mid k \in X\}$ 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 смежные классы группы (X, \otimes) по некоторой 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 вытекает существование подстановочного гомоморфизма $\tilde{\varphi}_{\mathbf{W}}$ — естественного гомоморфизма импримитивной группы G в симметрическую группу, действующую на множестве номеров блоков $\{0, \dots, r-1\}$, который однозначно задается отображением $\varphi_{\mathbf{W}}: X \rightarrow \{0, \dots, r-1\}$, удовлетворяющим условию

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

В общем случае наличие подстановочного гомоморфизма $\tilde{\varphi}_{\mathbf{W}}$ группы G не обеспечивает существование гомоморфизма θ алгоритма $C_l(\otimes, b)$.

В настоящей работе показано, что из условий $\otimes_{\mathbf{W}}$ — марковости алгоритма $C_l(\otimes, b)$ и абелевости группы (X, \otimes) следует, что подстановочный гомоморфизм $\tilde{\varphi}_{\mathbf{W}}$ группы G однозначно определяет гомоморфизм θ алгоритма $C_l(\otimes, b)$, а именно, $\theta = \varphi_{\mathbf{W}}$. Такой гомоморфизм θ алгоритма $C_l(\otimes, b)$ будем также называть подстановочным.

Для алгебраического подхода естественным является рассмотрение разбиения \mathbf{W} , блоки которого являются смежными классами по некоторой подгруппе группы (X, \otimes) . В этом случае блок $W_0 \in \mathbf{W}$, где $e \in W_0$, $|W_0| \geq 2$, соответствует поглощающему состоянию на языке теории цепей Маркова. Если блоки разбиения $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ не являются смежными классами по некоторой подгруппе (W_0, \otimes) группы (X, \otimes) , в частности неравномошны, то у $\otimes_{\mathbf{W}}$ -марковского алгоритма может не существовать подстановочного гомоморфизма $\tilde{\varphi}_{\mathbf{W}}$. В этом случае часто $W_0 = \{e\}$.

В [19] будут рассмотрены вопросы $\otimes_{\mathbf{W}}$ -марковости XSL-алгоритмов блочного шифрования, связанные со свойствами слоев раундовой функции.

2. Основные обозначения и понятия

В работе используются следующие обозначения: X — произвольное конечное множество; $S(X)$ — симметрическая группа на X ; (X, \otimes) — произвольная абелева группа на множестве X с бинарной операцией \otimes и единичным элементом e ; $X^\times = X \setminus \{e\}$; $\alpha^g = \alpha g = g(\alpha)$ — образ элемента $\alpha \in X$ при действии на него подстановкой $g \in S(X)$; α^{-1} — обратный к α элемент относительно операции \otimes , $\alpha \bar{\otimes} \beta = \alpha \otimes \beta^{-1}$ для любых $\alpha, \beta \in X$; K — множество всех раундовых ключей; $g: (\alpha, k) \mapsto g(\alpha, k)$ — раундовая функция, а $g_k: \alpha \mapsto g(\alpha, k)$ — частичная раундовая функция, $(\alpha, k) \in X \times K$; $f_{\vec{k}_t} = g_{k_1} \dots g_{k_t}$ для $\vec{k}_t = (k_1, \dots, k_t) \in K^t$; $V_m = V_m(2)$ — векторное пространство размерности m над полем $GF(2)$; \oplus — операция покомпонентного сложения векторов над полем $GF(2)$; $\langle \delta_1, \dots, \delta_c \rangle$ — группа, порожденная элементами $\delta_1, \dots, \delta_c$; $I(A)$ — индикатор выполнения условия A ;

$\vec{0}_n$ — n -мерный нулевой вектор; $G_1 \wr G_2$ — сплетение групп подстановок G_1, G_2 ; $\mathbf{W}_{w,r}(X)$ — множество всех разбиений X с r блоками мощности w каждый, $|X| = wr$, $w > 1$, $r > 1$; $\text{IGW} = (S_w \wr S_r, \mathbf{W})$ — максимальная группа подстановок, сохраняющая разбиение $\mathbf{W} \in \mathbf{W}_{w,r}(X)$; V_n^+ ($\mathbb{Z}_{2^n}^+$) — регулярное подстановочное представление группы сдвигов пространства V_n (аддитивной группы кольца \mathbb{Z}_{2^n}).

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

$$\begin{aligned} p_{\theta, \varepsilon}(g) &= \frac{1}{|K||X|} |\{(\alpha, k) \in X \times K \mid (\theta \otimes \alpha)^{gk} = \varepsilon \otimes \alpha^{gk}\}|, \\ p_{\theta, \varepsilon}(g|\beta) &= \frac{1}{|K|} |\{k \in K \mid (\theta \otimes \beta)^{gk} = \varepsilon \otimes \beta^{gk}\}|, \quad \beta \in X, \\ \hat{p}_{\theta, \varepsilon}(b) &= \frac{1}{|X|} |\{\alpha \in X \mid (\theta \otimes \alpha)^b = \varepsilon \otimes \alpha^b\}|, \end{aligned}$$

$\mathbf{p}(g) = (p_{\theta, \varepsilon}(g))$ — матрица вероятностей переходов разностей 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 $\zeta_{\mathbf{U}}^{(0)}, \zeta_{\mathbf{U}}^{(1)}, \dots, \zeta_{\mathbf{U}}^{(t)}, \dots$ на множестве $\{0, \dots, r-1\}$, что $\zeta_{\mathbf{U}}^{(t)} = j$ тогда и только тогда, когда $\zeta^{(t)} \in U_j$, где $j \in \{0, \dots, r-1\}, t = 0, 1, \dots$

Определение 1 ([16]). 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 $\zeta_{\mathbf{U}}^{(0)}, \zeta_{\mathbf{U}}^{(1)}, \dots, \zeta_{\mathbf{U}}^{(t)}$ 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 $g: X^2 \mapsto X$ 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

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

т. е. 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 $\xi^{(0)}$ со значениями в 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 $\alpha \in X$, если раундовые ключи k_1, \dots, k_l независимо и равновероятно выбираются 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.

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

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

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

Раундовой функции g $\otimes_{\mathbf{W}}$ -марковского алгоритма блочного шифрования поставим 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

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

Определение 4 ([2]). Будем говорить, что преобразование $b \in S(X)$ является $\otimes_{\mathbf{W}}$ -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 каждых $(j, c) \in \{0, \dots, r-1\}^2, \theta \in W_j$, и некоторых $a_{j,c}, 0 \leq a_{j,c} \leq 1$.

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

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

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

Для $W_t \in \mathbf{W}$ положим $W_t = \{\theta_1^{(t)}, \dots, \theta_{w_t}^{(t)}\}$ при $t = 0, \dots, r-1$, $w_t = |W_t|$, $r = |\mathbf{W}|$. Произвольной паре блоков $(W_i, W_j) \in \mathbf{W}^2$ поставим в соответствие $(w_i \times w_j)$ -матрицу $\mathbf{p}_{W_i, W_j}(g) = (p_{\theta_t^{(i)}, \theta_c^{(j)}}(g))$. Заметим, что из условий $\otimes_{\mathbf{W}}$ -марковости алгоритма $C_l(\otimes, b)$ вытекает равенство суммы всех элементов каждой строки матрицы $\mathbf{p}_{W_i, W_j}(g)$ элементу $p_{W_i, W_j}(g)$ матрицы $\mathbf{p}_{\mathbf{W}}(g)$. Очевидно, что матрица $\mathbf{p}(g)$ подобна (относительно перестановки строк и столбцов) матрице вида

$$\begin{pmatrix} \mathbf{p}_{W_0, W_0}(g) & \cdots & \mathbf{p}_{W_0, W_{r-1}}(g) \\ \vdots & \cdots & \vdots \\ \mathbf{p}_{W_{r-1}, W_0}(g) & \cdots & \mathbf{p}_{W_{r-1}, W_{r-1}}(g) \end{pmatrix}.$$

Определение 5. Пусть Y — произвольное конечное множество. Объединением разбиения $\mathbf{W} = \{W_0, \dots, W_{d-1}\}$ множества Y называется разбиение $\mathbf{W}' = \{W'_0, \dots, W'_{d'-1}\}$, блоки которого являются объединениями блоков разбиения \mathbf{W} , т. е. $W'_c = \bigcup_{i \in J_c} W_i$ для некоторого разбиения $J = \{J_0, \dots, J_{d'-1}\}$ множества $\{0, \dots, d-1\}$.

Определение 6. Назовем разбиение \mathbf{W} множества X нетривиальным, если $\mathbf{W} \notin \{\{\{\alpha\} | \alpha \in X\}, \{X\}\}$.

Определение 7. Подстановочным гомоморфизмом будем называть естественный гомоморфизм импримитивной группы G с системой импримитивности $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ в симметрическую группу $S(\{0, \dots, r-1\})$.

3. Гомоморфизмы и $\otimes_{\mathbf{W}}$ -марковость

В данном разделе для произвольной абелевой 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.

Пусть X^\otimes — регулярная группа подстановок на множестве X . Ее элементом является подстановка $\sigma_k \in X^\otimes$, заданная условием $\sigma_k: x \mapsto x \otimes k$ для $k \in X$. Ясно, что $g_k = \sigma_k b$ для каждого $k \in X$. Заметим, что для алгоритма $C_l(\otimes, b)$ справедливо равенство $\widehat{\mathbf{p}}(b) = \mathbf{p}(g)$.

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

Пусть $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ — разбиение множества X , $e \in W_0$. 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 некоторого $i \in \{0, \dots, r-1\}$.

Произвольная бинарная операция $\tilde{\odot}$ на множестве $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ естественным образом индуцирует бинарную операцию \odot на множестве $\{0, \dots, r-1\}$ условием

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

Заметим, что $(\mathbf{W}, \tilde{\odot})$ – группоид, а бинарная операция $\tilde{\odot}$ может быть задана посредством таблицы Кэли для группоида (см., например, [17]). Очевидно, что если операция $\tilde{\odot}$ на \mathbf{W} индуцируется групповой операцией \otimes на X посредством равенства

$$W \otimes W' = \{\alpha \otimes \alpha' \mid (\alpha, \alpha') \in W \times W'\} \quad \text{для всех } W, W' \in \mathbf{W},$$

то бинарная операция $\tilde{\odot}$ ($\tilde{\odot} = \otimes$) на \mathbf{W} , а тем самым и \odot на $\{0, \dots, r-1\}$, определены корректно только при таком условии, что $(W_0, \otimes) \trianglelefteq (X, \otimes)$ и W_j – j -й смежный класс группы (X, \otimes) по подгруппе (W_0, \otimes) для $j = 0, \dots, r-1$.

Для произвольной подстановки $b \in S(X)$, сохраняющей разбиение \mathbf{W} , определим подстановку $\bar{b} \in S(\{0, \dots, r-1\})$ условием

$$(\varphi_{\mathbf{W}}(\alpha))^{\bar{b}} = \varphi_{\mathbf{W}}(\alpha^b) \quad \text{для каждого } \alpha \in X. \quad (3)$$

В следующей теореме показывается, что условие $\otimes_{\mathbf{W}}$ -марковости алгоритма $C_l(\otimes, b)$ эквивалентно существованию у него подстановочного гомоморфизма. 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. Пусть (X, \otimes) – произвольная абелева группа, $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ – нетривиальное разбиение множества X , $e \in W_0$, $l \in \mathbb{N}$. Тогда следующие условия эквивалентны.

1. Разбиение $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ сохраняется множеством $\{g_k \mid k \in X\}$.
2. $\varphi_{\mathbf{W}}$ – гомоморфизм $C_l(\otimes, b)$ в $C_l(\odot, \bar{b})$, причем в алгоритме $C_l(\odot, \bar{b})$ корректно определены бинарная операция \odot на $\{0, \dots, r-1\}$, индуцированная групповой операцией \otimes на X , и подстановка \bar{b} , заданные соответственно условиями (2) (при $\tilde{\odot} = \otimes$) и (3).
3. W_j – j -й смежный класс группы (X, \otimes) по подгруппе (W_0, \otimes) при $j = 0, \dots, r-1$, а $C_l(\otimes, b)$ является $\otimes_{\mathbf{W}}$ -марковским.

Доказательство. $1 \Rightarrow 2$. Так как g_{k_1}, g_{k_2} сохраняют разбиение \mathbf{W} на любых $k_1, k_2 \in X$, 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

$$\mathbf{W}^{X^\otimes} = \mathbf{W}. \quad (4)$$

Кроме того,

$$\mathbf{W}^{g_e} = \mathbf{W}^b = \mathbf{W}. \quad (5)$$

Таким образом, подстановка \bar{b} корректно задана условием (3). Из равенств (4), (5), а также из транзитивности группы X^\otimes следует, что группа $\langle b, X^\otimes \rangle$ импримитивна с системой импримитивности \mathbf{W} . Кроме того, из импримитивности группы X^\otimes вытекает справедливость включения $W_0 \otimes k \in \mathbf{W}$ для каждого $k \in X$ тогда и только тогда, когда $(W_0, \otimes) \triangleleft (X, \otimes)$, а W_j — j -й смежный класс группы (X, \otimes) по (W_0, \otimes) . Очевидно, что из нормальности $(W_0, \otimes) \triangleleft (X, \otimes)$ вытекает корректность задания бинарной операции \odot на множестве $\{0, \dots, r-1\}$, индуцированной групповой операцией \otimes на X и заданной условием (2) (при $\tilde{\odot} = \otimes$).

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

$$\begin{aligned} \bar{g}_{\varphi_{\mathbf{W}}(k)}(\varphi_{\mathbf{W}}(\alpha)) &= \varphi_{\mathbf{W}}(g_k(\alpha)) = \\ &= \varphi_{\mathbf{W}}((\alpha \otimes k)^b) = (\varphi_{\mathbf{W}}(\alpha \otimes k))^{\bar{b}} = \\ &= (\varphi_{\mathbf{W}}(\alpha) \odot \varphi_{\mathbf{W}}(k))^{\bar{b}} \end{aligned} \quad (6)$$

для всех $(\alpha, k) \in X^2$. Из равенства (6) вытекает, что $\varphi_{\mathbf{W}}$ — гомоморфизм $C_l(\otimes, b)$ в $C_l(\odot, \bar{b})$.

$2 \Rightarrow 3$. Пусть отображение $\varphi_{\mathbf{W}}$ — гомоморфизм $C_l(\otimes, b)$ в $C_l(\odot, \bar{b})$. Из корректности заданий бинарной операции \odot на $\{0, \dots, r-1\}$, заданной условием (2) (при $\tilde{\odot} = \otimes$) и индуцированной групповой операцией \otimes на X , и подстановки \bar{b} , определенной условием (3), вытекает:

1. W_j — j -й смежный класс группы $(X, \otimes)(W_0, \otimes)$ для $j=0, \dots, r-1$.
2. $\mathbf{W}^b = \mathbf{W}$.

Отсюда и из справедливости равенства $\theta \otimes W_j = W_{c \odot j}$ для каждого $c, j \in \{0, \dots, r-1\}$, $\theta \in W_c$ следуют условия

$$(\theta \otimes W_j)^b \bar{\otimes} W_j^b = W_{u_{c,j}}, (\theta \otimes \beta)^b \bar{\otimes} \beta^b \in W_{u_{c,j}}, \quad (7)$$

выполняющиеся для каждого $\beta \in W_j$ и некоторых $u_{c,j} \in \{0, \dots, r-1\}$.

Из условий (7) следуют равенства

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

для $t = 0, \dots, r-1$. Из определения 3 вытекает $\otimes_{\mathbf{W}}$ -марковость алгоритма $C_l(\otimes, b)$.

3 \Rightarrow 1. Предположим теперь $\otimes_{\mathbf{W}}$ -марковость алгоритма $C_l(\otimes, b)$, где $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ – множество смежных классов группы (X, \otimes) по подгруппе (W_0, \otimes) . Так как $p_{e, W_0}(g) = 1$, то $p_{\theta, W_0}(g) = 1$ для каждого $\theta \in W_0$, что эквивалентно

$$(W_0 \otimes \alpha)^b = W_0 \otimes \alpha^b \quad \text{для каждого } \alpha \in X.$$

Отсюда вытекает равенство

$$(W_0 \otimes \alpha)^b = W_0^{g\alpha} = W_0 \otimes \alpha^b \quad \text{для каждого } \alpha \in X. \quad (8)$$

Из равенства (8) следует, что множество $\{g_k | k \in X\}$ сохраняет разбиение \mathbf{W} . \square

Из доказательства теоремы следует, что если разбиение $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ сохраняется множеством $\{g_k | k \in X\}$, то $(W_0, \otimes) \leq (X, \otimes)$, а W_j – j -й смежный класс группы (X, \otimes) по (W_0, \otimes) . Также заметим, что из импримитивности группы $G = \langle b, X^{\otimes} \rangle$ следуют включения

$$b \in \text{IG}_{\mathbf{W}}, \quad \langle g_k | k \in X \rangle \leq \text{IG}_{\mathbf{W}}, \quad \langle g_{k_1} \cdots g_{k_l} | (k_1, \dots, k_l) \in X^l \rangle \leq \text{IG}_{\mathbf{W}}.$$

Возможны ситуации, при которых группа $\langle b, X^{\otimes} \rangle$ примитивна. Ясно, что тогда множество $\{g_k | k \in X\}$ не сохраняет никакого нетривиального разбиения множества X .

Из теоремы следует, что $\mathbf{p}_{\mathbf{W}}(g) = \mathbf{p}(\bar{g})$, где $\bar{g}: \{0, \dots, r-1\}^2 \rightarrow \{0, \dots, r-1\}$ — раундовая функция алгоритма $C_l(\odot, \bar{b})$, а $\mathbf{p}_{\mathbf{W}}(g)$ — матрица вероятностей переходов укрупненной марковской цепи $\xi_{\mathbf{W}}^{(0)}, \dots, \xi_{\mathbf{W}}^{(l)}$. Заметим, что матрица $\mathbf{p}_{\mathbf{W}}(g)$ может не быть подстановочной.

Из включения $e \in W_0$ вытекает равенство $p_{W_0, W_0}(g) = p_{0,0}(\bar{g}) = 1$. Поэтому состояние W_0 марковской цепи $\xi_{\mathbf{W}}^{(0)}, \dots, \xi_{\mathbf{W}}^{(l)}$ является поглощающим. В общем случае для дальнейшего изучения свойств марковской цепи $\xi_{\mathbf{W}}^{(0)}, \dots, \xi_{\mathbf{W}}^{(l)}$ необходимо использовать дополнительные свойства преобразования b .

Неявно допущение о $\otimes_{\mathbf{W}}$ -марковости алгоритма блочного шифрования для некоторого класса упорядоченных наборов используется в методе усеченных разностей (см. [12–15]). В этом случае вместо вероятности $p_{W_0, W_0}(g)$ для оценки трудоемкости метода используется вероятность $p_{W_0 \setminus \{e\}, W_0 \setminus \{e\}}(g)$.

Согласно теореме условие сохранения разбиения \mathbf{W} множеством $\{g_k | k \in X\}$ накладывает сильные ограничения на структуру разбиения \mathbf{W} . Из данных ограничений следует эквивалентность $\otimes_{\mathbf{W}}$ -марковости алгоритма $C_l(\otimes, b)$ существованию отображения $\varphi_{\mathbf{W}}$, задающего гомоморфизм $C_l(\otimes, b)$ в $C_l(\odot, \bar{b})$. Если не требовать сохранения разбиения \mathbf{W} множеством $\{g_k | k \in X\}$, то могут существовать такие преобразования b , что алгоритм $C_l(\otimes, b)$ является $\otimes_{\mathbf{W}}$ -марковским, а группа $\langle g_k | k \in X \rangle$ примитивна. Такие преобразования будут описаны в [19].

Приведем для $\otimes_{\mathbf{W}}$ -марковского алгоритма блочного шифрования с раундовой функцией g множество $\otimes_{\mathbf{W}}$ -марковских алгоритмов блочного шифрования, раундовые функции которых связаны с g посредством группы $\text{IG}_{\mathbf{W}}$.

Следствие. Пусть разбиение $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ множества X таково, что:

- 1) W_j — j -й смежный класс группы (X, \otimes) по подгруппе (W_0, \otimes) для $j=0, \dots, r-1$;
- 2) алгоритм блочного шифрования с раундовой функцией $g : X \times K \rightarrow X$ является $\otimes_{\mathbf{W}}$ -марковским;
- 3) v — произвольная подстановка из $\text{IG}_{\mathbf{W}}$.

Тогда алгоритмы блочного шифрования, у которых раундовые функции $g^{[v]} : X \times K \rightarrow X$, $g'^{[v]} : X \times K \rightarrow X$ заданы условиями

$$g^{[v]} : (x, k) \mapsto x^{vg_k}, \quad g'^{[v]} : (x, k) \mapsto x^{g_k v},$$

являются $\otimes_{\mathbf{W}}$ -марковскими.

Доказательство следует из теоремы. □

Множество всех нетривиальных разбиений на смежные классы, задаваемых подгруппами группы (X, \otimes) , обозначим

$$N_{\otimes}(X) = \{ \{B \otimes \delta \mid \delta \in X\} \mid \{e\} < B < X \}.$$

Теорема устанавливает для алгоритма $C_l(\otimes, b)$ соответствие между $\otimes_{\mathbf{W}}$ -марковостью и существованием подстановочного гомоморфизма $\varphi_{\mathbf{W}}$ для разбиений \mathbf{W} из множества $N_{\otimes}(X)$.

Рассмотрим далее группу $(X, \otimes) \in \{(V_n, \oplus), (\mathbb{Z}_{2^n}, +)\}$, т. е. X^+ совпадает с одной из двух наиболее часто встречающихся в алгоритмах блочного шифрования группами наложения ключа $V_n^+, \mathbb{Z}_{2^n}^+$. Для разбиения $\mathbf{W} \notin N_{\otimes}(X)$ в утверждении 1 опишем класс таких $\otimes_{\mathbf{W}}$ -марковских алгоритмов $C_l(\otimes, b)$, что $\{g_k \mid k \in X\}$ является подмножеством смежного класса по импримитивной подгруппе $IG_{\mathbf{U}}$ группы $S(X)$ для некоторого разбиения $\mathbf{U} \in N_{\otimes}(X)$. Тем самым даже при $\mathbf{W} \notin N_{\otimes}(X)$ существуют $\otimes_{\mathbf{W}}$ -марковские алгоритмы $C_l(\otimes, b)$, для анализа которых можно попытаться применить метод гомоморфизмов с гомоморфизмом $\varphi_{\mathbf{U}}$. Приведем сначала пример для группы $X^+ = V_n^+$.

Пусть $IG_{\mathbf{W}}$ — максимальная группа подстановок, сохраняющая разбиение \mathbf{W} ; $\text{rang } U$ — наибольшее число линейно независимых векторов множества $U \subseteq V_n$; $\langle U \rangle$ — подпространство V_n , порожденное множеством U .

Утверждение 1. Пусть $b \in S(V_n)$, g — раундовая функция алгоритма $C_l(\oplus, b)$ и существуют такие подмножества $W, W' \subset V_n$, что $p_{\beta, W'}(g) = 1$ для каждого $\beta \in W$ и $\text{rang } W = \text{rang } W' < n$. Тогда:

1. $b \in IG_{\mathbf{U}^a}$, $\{g_k \mid k \in V_n\} \subseteq IG_{\mathbf{U}^a}$, где $\mathbf{U} = \{\alpha \oplus \langle W \rangle \mid \alpha \in V_n\}$, a — такая произвольная подстановка из $S(V_n)$, что

$$\mathbf{U}^a = \mathbf{U}' = \{\alpha \oplus \langle W' \rangle \mid \alpha \in V_n\}.$$

Кроме того, если $\mathbf{U} = \mathbf{U}'$, то

$$b \in IG_{\mathbf{U}} \quad \langle g_k \mid k \in V_n \rangle \leq IG_{\mathbf{U}},$$

а $C_l(\oplus, b)$ — $\oplus_{\mathbf{U}}$ -марковский алгоритм.

2. Если $p_{\beta, W}(g) = 1$ для каждого $\beta \in W'$ и $W \cap W' = \{\emptyset, W\}$, то алгоритм $C_l(\oplus, b)$ является $\oplus_{\mathbf{W}}$ -марковским относительно разбиения $\mathbf{W} = \{W, W', V_n \setminus (W \cup W')\}$. Кроме того, $\mathbf{W} \notin N_{\oplus}(V_n)$, если выполнено одно из условий:

- 1) $\text{rang } W \neq n - 1$,
- 2) $\text{rang } W = n - 1$, $W \neq \langle W \rangle$.

Доказательство. 1. Равенство $p_{\beta, W'}(g) = 1$ для каждого $\beta \in W$ равносильно тому, что

$$(\alpha \oplus W)^b = \alpha^b \oplus W' \quad \text{для каждого } \alpha \in V_n. \quad (9)$$

Докажем, что из равенства (9) вытекает равенство

$$(\alpha \oplus \langle W \rangle)^b = \alpha^b \oplus \langle W' \rangle \quad \text{для каждого } \alpha \in V_n.$$

Ясно, что $|W| = |W'|$. Пусть $W = \{\omega_1, \dots, \omega_r\}$, $W' = \{\omega'_1, \dots, \omega'_r\}$. Так как $V_n = \langle W \rangle \oplus U$ для некоторого подпространства $U < V_n$, $\langle W \rangle \cap U = \{\vec{0}_n\}$, то любой элемент из V_n представим в виде $\beta \oplus \omega$, где $\beta \in U$, $\omega \in \langle W \rangle$.

Зафиксируем произвольный элемент $\beta \in U$. Тогда из равенства (9) следует существование подстановки $q_\beta \in S(\{0, \dots, r-1\})$, удовлетворяющей равенствам

$$(\beta \oplus \omega_j)^b = \beta^b \oplus \omega'_{q_\beta(j)}, \quad j = 0, \dots, r-1. \quad (10)$$

Из равенств (9), (10) вытекает, что для любых $j_1, j_2 \in \{0, \dots, r-1\}$, $j_1 \neq j_2$, справедливо равенство

$$\begin{aligned} (\beta \oplus \omega_{j_1} \oplus \omega_{j_2})^b &= (\beta \oplus \omega_{j_1})^b \oplus \omega'_{q_{\beta \oplus \omega_{j_1}}(j_2)} = \\ &= \beta^b \oplus \omega'_{q_\beta(j_1)} \oplus \omega'_{q_{\beta \oplus \omega_{j_1}}(j_2)} = \beta^b \oplus \omega'_{q_\beta(j_2)} \oplus \omega'_{q_{\beta \oplus \omega_{j_2}}(j_1)}. \end{aligned}$$

Значит, $\omega'_{q_{\beta \oplus \omega}(j)} = \omega'_{q_\beta(j)}$ для всех $j \in \{0, \dots, r-1\}$, $\omega \in W$. Поэтому

$$(\beta \oplus \omega_{j_1} \oplus \omega_{j_2})^b = \beta^b \oplus \omega'_{q_\beta(j_1)} \oplus \omega'_{q_\beta(j_2)}.$$

Аналогично, с помощью индукции по числу $d \in \{2, \dots, r\}$, доказывается справедливость равенства

$$(\beta \oplus \omega_{j_1} \oplus \dots \oplus \omega_{j_d})^b = \beta^b \oplus \omega'_{q_\beta(j_1)} \oplus \dots \oplus \omega'_{q_\beta(j_d)} \quad (11)$$

для любых $j_1, \dots, j_d \in \{0, \dots, r-1\}$. Таким образом,

$$(\alpha \oplus \langle W \rangle)^b = \alpha^b \oplus \langle W' \rangle \quad \text{для каждого } \alpha \in V_n.$$

Значит, справедливо равенство $\mathbf{U}^b = \mathbf{U}'$, т. е.

$$b \in \text{IG}_{\mathbf{U}.a}, \quad \{g_k | k \in V_n\} \subseteq \text{IG}_{\mathbf{U}} a.$$

Если $\mathbf{U} = \mathbf{U}'$, то из утверждения 1.2.1 [18] следуют включения

$$b \in \text{IG}_{\mathbf{U}}, \quad \langle g_k | k \in V_n \rangle \leq \text{IG}_{\mathbf{U}}.$$

2. Непосредственно вытекает из утверждения 3 [2]. \square

Приведем аналог утверждения 1 для $X^+ = \mathbb{Z}_{2^n}^+$.

Утверждение 2. Пусть

$$(X, \otimes) = (\mathbb{Z}_{2^n}, +), \quad b \in S(\mathbb{Z}_{2^n}),$$

a, g — раундовая функция алгоритма $C_l(+, b)$. Пусть существуют такие подмножества $W, W' \subset \{0, \dots, 2^n - 1\}$, что

$$p_{\beta, W'}(g) = 1 \quad \text{для каждого } \beta \in W,$$

$\langle W \rangle = \langle W' \rangle$ и $\langle W \rangle < (\mathbb{Z}_{2^n}, +)$. Тогда:

1. Для разбиения $\mathbf{U} = \{\alpha + \langle W \rangle \mid \alpha \in \mathbb{Z}_{2^n}\}$ справедливы включения

$$b \in \text{IG}_{\mathbf{U}}, \langle g_k \mid k \in \mathbb{Z}_{2^n} \rangle \leq \text{IG}_{\mathbf{U}},$$

а алгоритм $C_l(+, b)$ является $+\mathbf{U}$ -марковским.

2. Если

$$p_{\beta, W}(g) = 1 \quad \text{для каждого } \beta \in W'$$

и $W \cap W' = \{\emptyset, W\}$, то алгоритм $C_l(+, b)$ является $+\mathbf{W}$ -марковским относительно разбиения

$$\mathbf{W} = \{W, W', \{0, \dots, 2^n - 1\} \setminus (W \cup W')\}.$$

Кроме того, $\mathbf{W} \notin N_+(\mathbb{Z}_{2^n})$, если $|W| \neq 2^{n-1}$.

Доказательство аналогично доказательству утверждения 1. □

Заметим, что достаточным условием для выполнения равенства $\langle W \rangle = \langle W' \rangle$ является равенство мощностей в силу единственности подгруппы данного порядка в группе $\mathbb{Z}_{2^n}^+$. Так как у группы V_n^+ имеется большое число подгрупп мощности 2^t , то в формулировке утверждения 1 присутствует равенство $\text{rang } W = \text{rang } W'$, являющееся более слабым условием по сравнению с условием $\langle W \rangle = \langle W' \rangle$ утверждения 2.

Очевидно, что каждая подстановка из $S(V_n)$ является $\oplus_{\mathbf{W}}$ -марковской для разбиения $\mathbf{W} = \{\{\vec{0}_n\}, V_n^\times\}$. Для таких разбиений \mathbf{W} пространства V_n с двумя блоками, что $\mathbf{W} \neq \{\{\vec{0}_n\}, V_n^\times\}$, опишем классы $\oplus_{\mathbf{W}}$ -марковских подстановок.

Утверждение 3. Пусть $n \geq 2$ и разбиение $\mathbf{W} = \{W_0, W_1\}$ пространства V_n таково, что $\vec{0}_n \in W_0$, $2 \leq |W_0| \leq 2^n - 2$. Тогда каждая $\oplus_{\mathbf{W}}$ -марковская подстановка $s \in S(V_n)$ удовлетворяет включению

$$s \in \text{IG}_{\mathbf{W}^{(i)}}, \quad \text{где } \mathbf{W}^{(i)} = \{W_0^{(i)}, \dots, W_{r^{(i)}-1}^{(i)}\},$$

а $W_0^{(i)}$ — j -й смежный класс по подпространству $W_0^{(i)} = \langle W_i \rangle$ для $i = 0, 1$.

Доказательство. Без ограничения общности предположим, что $\vec{0}_n \in W_0$. Так как $\widehat{p}_{\vec{0}_n, W_0}(s) = \widehat{p}_{\vec{0}_n, \vec{0}_n}(s) = 1$, то для каждого $\theta \in W_0$ выполняется равенство

$$\widehat{p}_{\theta, W_0}(s) = \sum_{\theta' \in W_0} \widehat{p}_{\theta, \theta'}(s) = 1,$$

из которого следует, что

$$\widehat{p}_{\theta, W_1}(s) = \sum_{\theta' \in W_1} \widehat{p}_{\theta, \theta'}(s) = 0. \quad (12)$$

Значит, для каждого $\alpha \in V_n$ имеем

$$(\alpha \oplus W_0)^s = \alpha^s \oplus W_0, \quad (\alpha \oplus W_1)^s = \alpha^s \oplus W_1,$$

в частности $W_0^s = \vec{0}_n^s \oplus W_0$, $W_1^s = \vec{0}_n^s \oplus W_1$ (при $\alpha = \vec{0}_n$). Отсюда следует, что для каждого $t \in \mathbb{N}$, $i \in \{0, 1\}$ выполняются равенства

$$\begin{aligned} \left(\underbrace{W_i \oplus \dots \oplus W_i}_t \right)^s &= \left(\underbrace{W_i \oplus \dots \oplus W_i}_{t-1} \right)^s \oplus W_i = \\ &= \vec{0}_n^s \oplus \underbrace{W_i \oplus \dots \oplus W_i}_t. \end{aligned}$$

Отсюда и из равенства (12) вытекает, что для каждого $\alpha \in V_n$ справедливы равенства

$$(\alpha \oplus \langle W_0 \rangle)^s = \alpha^s \oplus \langle W_0 \rangle, \quad (\alpha \oplus \langle W_1 \rangle)^s = \alpha^s \oplus \langle W_1 \rangle.$$

Тогда из утверждения 1.2.1 [18] следуют включения $s \in \text{IG}_{\mathbf{W}^{(i)}}$, где $\mathbf{W}^{(i)}$ — множество всех смежных классов пространства V_n по подпространству $\langle W_i \rangle$ для $i = 0, 1$. \square

Заметим, что если в утверждении 3 блоки разбиения $\mathbf{W} = \{W_0, W_1\}$ таковы, что $\langle W_0 \rangle = \langle W_1 \rangle$, то

$$\text{rang } \langle W_0 \rangle = \text{rang } \langle W_1 \rangle = n.$$

Таким образом, если $\langle W_0 \rangle \neq \langle W_1 \rangle$, $\{\vec{0}_n\} \subset W_0 \subset V_n$, то для некоторого $i \in \{0, 1\}$ блок разбиения $\mathbf{W} = \{W_0, W_1\}$ удовлетворяет условию $1 \leq \text{rang } \langle W_i \rangle \leq n-1$. Следовательно, для каждого разбиения $\mathbf{W} = \{W_0, W_1\}$, где $\langle W_0 \rangle \neq \langle W_1 \rangle$, $\{\vec{0}_n\} \subset W_0 \subset V_n$, множество всех $\oplus_{\mathbf{W}}$ -марковских подстановок $s \in S(V_n)$ принадлежит некоторому нетривиальному сплетению групп.

В разделе 2 [19] будут указаны такие APN-подстановки и разностно 4-равномерные подстановки, которые не являются $\oplus_{\mathbf{W}}$ -марковскими для каждого разбиения $\mathbf{W} = \{W_0, W_1\}$ пространства V_n , удовлетворяющего условию $\langle W_0 \rangle \neq \langle W_1 \rangle$, $\{\vec{0}_n\} \subset W_0 \subset V_n$. Однако для этих подстановок приведены примеры разбиений \mathbf{W}' пространства V_n , $|\mathbf{W}'| \geq 3$, относительно которых они $\oplus_{\mathbf{W}'}$ -марковские.

Авторы выражают благодарность И. А. Круглову за ценные замечания.

Список литературы

- [1] Lai X., Massey J.L., Murphy S., "Markov ciphers and differential cryptanalysis", In: EUROCRYPT'1991, Lect. Notes Comput. Sci., **547**, 1991, 17–38.
- [2] Погорелов Б. А., Пудовкина М. А., "Разбиения на биграмах и марковость алгоритмов блочного шифрования", *Математические вопросы криптографии*, **8**:1 (2017), 5–40.
- [3] Knudsen L. R., Mathiassen J. E., "On the role of key schedules in attacks on iterated ciphers", In: ESORICS 2004, Lect. Notes Comput. Sci., **3193**, 2004, 322–334.
- [4] Hornauer G., Stephan W., Wernsdorf R., "Markov ciphers and alternating groups", In: EUROCRYPT'1993, Lect. Notes Comput. Sci., **765**, 1993, 453–460.
- [5] Сачков В. Н., "Вероятностные преобразователи и правильные мультиграфы. I", *Труды по дискретной математике*, **1** (1997), 227–250.
- [6] Сачков В. Н., "Цепи Маркова итерационных систем преобразований", *Труды по дискретной математике*, **6** (2002), 165–183.
- [7] Сачков В. Н., "Вероятностные преобразователи и суммы элементарных матриц. II", *Труды по дискретной математике*, **8** (2005), 240–252.
- [8] Ковальчук Л. В., "Обобщенные марковские шифры: построение оценок практической стойкости к дифференциальным атакам", В сб.: Математика и безопасность информационных технологий (МАБИТ). М.: МЦНМО, 2006.
- [9] Лисицкая И. В., Долгов В. И., "Блочные симметричные шифры и марковские процессы", *Прикладная радиоэлектроника*, **11**:2 (2012), 137–143.
- [10] Максимов Ю. И., "Некоторые результаты для задачи укрупнения состояний цепей Маркова", *Труды по дискретной математике*, **8** (2005), 148–154.

- [11] Vaudenay S., “On the Lai–Massey Scheme”, In: ASIACRYPT’1999, Lect. Notes Comput. Sci., **1716**, 1999, 8–19.
- [12] Matsui M., Tokita T., “Cryptanalysis of a reduced version of the block cipher E2”, In: FSE 1999, Lect. Notes Comput. Sci., **1636**, 1999, 71–80.
- [13] Moriai S., Sugita M., Aoki K., Kanda M., “Security of E2 against truncated differential cryptanalysis”, In: SAC 1999, Lect. Notes Comput. Sci., **1758**, 2000, 106–117.
- [14] Reichardt B., Wagner D., “Markov truncated differential cryptanalysis of Skipjack”, In: SAC 2002, Lect. Notes Comput. Sci., **2595**, 2003, 110–128.
- [15] Blondeau C., “Improbable differential from impossible differential: on the validity of the model”, In: INDOCRYPT 2013, Lect. Notes Comput. Sci., **8250**, 2013, 149–160.
- [16] Кемени Д., Снелл Д., *Конечные цепи Маркова*, М.: Наука, 1970, 272 с.
- [17] Глухов М. М., Елизаров В. П., Нечаев А. А., *Алгебра*, в 2 т., Т. II., М.: Гелиос АРВ, 2003.
- [18] Погорелов Б. А., Пудовкина М. А., “Факторструктуры преобразований”, *Математические вопросы криптографии*, **3:3** (2012), 81–104.
- [19] Погорелов Б. А., Пудовкина М. А., “ $\otimes_{\mathbb{W}}$ -марковость XSL-алгоритмов блочного шифрования, связанная со свойствами слоев раундовой функции”, *Математические методы криптографии*, **10** (2019), в печати.