Math-Net.Ru

Общероссийский математический портал

Б. А. Погорелов, М. А. Пудовкина, $\otimes$ **w**-марковость XSL-алгоритмов блочного шифрования, связанная со свойствами слоев раундовой функции, *Матем. вопр. криптогр.*, 2019, том 10, выпуск 1, 115–142

DOI: <https://doi.org/10.4213/mvk279>

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: 54.84.234.179

26 апреля 2023 г., 13:48:50

**$\otimes_{\mathbf{W}}$ -марковость XSL-алгоритмов
блочного шифрования, связанная
со свойствами слоев раундовой функции**

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

Переработанный вариант 4.XII.2018

Аннотация. Ранее авторами были описаны условия существования подстановочных гомоморфизмов для некоторого класса $\otimes_{\mathbf{W}}$ -марковских алгоритмов. В настоящей работе получены условия $\oplus_{\mathbf{W}}$ -марковости S -боксов и преобразования линейного слоя. В частности, приведено достаточное условие на S -боксы и преобразование линейного слоя, при которых XSL-алгоритм является $\oplus_{\mathbf{W}}$ -марковским.

Ключевые слова: марковский алгоритм блочного шифрования, цепи Маркова, укрупнение состояний, $\otimes_{\mathbf{W}}$ -марковость, XSL-алгоритм, разностно d -равномерное преобразование

$\otimes_{\mathbf{W}}$ -markovianity of XSL-block ciphers connected with properties of their round functions

B. A. Pogorelov¹, M. A. Pudovkina²

¹ Academy of Cryptography of the Russian Federation, Moscow

² Bauman Moscow State Technical University, Moscow

Abstract. Earlier we have described conditions for the existence of permutation homomorphisms for some class of a $\otimes_{\mathbf{W}}$ -markovian block ciphers. In this paper we give conditions on S -boxes and on linear transformations which guaranteeing the $\oplus_{\mathbf{W}}$ -markovian property. In particular, we provide sufficient conditions on these transformations under which the corresponding XSL-block cipher is $\oplus_{\mathbf{W}}$ -markovian.

Key words: Markov block cipher, Markov chain, lumped states, $\otimes_{\mathbf{W}}$ -markovian property, XSL-block cipher, differentially d -uniform transformation

Citation: *Matematicheskie Voprosy Kriptografii*, 2019, v. 10, № 1, pp. 115–142 (Russian)

© Академия криптографии Российской Федерации, 2019 г.

1. Введение

В [1] для итерационного алгоритма блочного шифрования с абелевой группой $(X, \otimes)$ наложения ключа, а также с независимыми и равновероятно выбираемыми из множества X раундовыми ключами введено понятие $\otimes$ -марковского алгоритма блочного шифрования. Для таких алгоритмов последовательность раундовых разностей является марковской цепью. В [2] приведены 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. В [2] также введено понятие $\otimes_{\mathbf{W}}$ -марковского преобразования, естественным образом следующее из определения $\otimes_{\mathbf{W}}$ -марковского алгоритма блочного шифрования. Матрица вероятностей переходов разностей $\otimes_{\mathbf{W}}$ -марковских преобразований имеет определенную структуру.

Далее рассматривается l -раундовый алгоритм блочного шифрования $C_l(\otimes, b)$, у которого частичная раундовая функция $g_k: X \rightarrow X$, определяемая подстановкой $b \in S(X)$ ($S(X)$ — симметрическая группа подстановок на множестве X), задана условием

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

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 $\vec{k}_l = (k_1, \dots, k_l) \in X^l$ определена условием $f_{\vec{k}_l}^{(l)} = g_{k_1} \cdots g_{k_l}$.

В [3] описаны ограничения на преобразование b , группу $(X, \otimes)$ и разбиение $\mathbf{W}$, при которых алгоритм $C_l(\otimes, b)$ является $\otimes_{\mathbf{W}}$ -марковским, а группа $G = \langle g_k \mid k \in X \rangle$ импримитивна с системой импримитивности $\mathbf{W}$. Указаны условия, при которых существование гомоморфизма алгоритма $C_l(\otimes, b)$ равносильно его $\otimes_{\mathbf{W}}$ -марковости.

Настоящая работа является продолжением [3]. В ней основное внимание уделено случаям, когда группа $(X, \otimes)$ совпадает с группой $(\mathbb{Z}_{2^n}, +)$ или с группой $(V_n(2), \oplus)$, которые чаще всего встречаются в качестве групп наложения ключа в алгоритмах блочного шифрования, где $\mathbb{Z}_{2^n}$ — кольцо вычетов по модулю 2^n , $V_n(2)$ — векторное пространство размерности n над полем $GF(2)$ с операцией $\oplus$ покоординатного сложения векторов над полем $GF(2)$.

Частным случаем алгоритмов типа $C_l(\oplus, b)$ являются XSL-алгоритмы блочного шифрования, в которых подстановка b представима в виде произведения двух подстановок s (нелинейного преобразования, реализуемого слоем S -боксов) и h (преобразования линейного слоя).

В общем случае выяснение того, является ли $\oplus$ -марковский алгоритм блочного шифрования $\oplus_{\mathbf{W}}$ -марковским, и указание соответствующего разбиения $\mathbf{W}$ — сложная задача. Для XSL-алгоритмов блочного шифрования в ряде случаев она может быть упрощена и сведена к выявлению $\oplus_{\mathbf{W}}$ -марковости у компонент раундовой функции (S -боксов и линейного преобразования h). Из $\oplus_{\mathbf{W}}$ -марковости одной из компонент раундовой функции не следует $\oplus_{\mathbf{W}}$ -марковость алгоритма $C_l(\oplus, sh)$. Однако при некоторых условиях из $\oplus_{\mathbf{W}}$ -марковости каждого из преобразований s , h вытекает $\oplus_{\mathbf{W}}$ -марковость алгоритма $C_l(\oplus, sh)$ (например, если тождественно хотя бы одно из преобразований s , h).

В настоящей работе описываются условия, при которых S -боксы и линейные преобразования являются $\oplus_{\mathbf{W}}$ -марковскими. Приведены условия на S -боксы и линейные преобразования, при выполнении которых имеет место $\oplus_{\mathbf{W}}$ -марковость XSL-алгоритма, причем условие на линейное преобразование равносильно его $\oplus_{\mathbf{W}}$ -марковости. Так, для ряда S -боксов (подстановок), в том числе и APN-подстановок, доказано, что свойство $\oplus_{\mathbf{W}}$ -марковости S -блока связано со свойствами орграфа $\bar{\Gamma}(s)$, задаваемого матрицей вероятностей переходов разностей подстановки s . Приведены примеры $\oplus_{\mathbf{W}}$ -марковских подстановок, не принадлежащих никакой импримитивной группе подстановок (такие подстановки можно рассматривать как «сильно примитивные» (см. [4, 5]). В связи с выявлением $\oplus_{\mathbf{W}}$ -марковости у преобразования линейного слоя в работе для произвольного аффинного преобразования $h \in AGL_n(2)$ описаны все нетривиальные разбиения $\mathbf{W}$ пространства $V_n(2)$, относительно которых h является $\oplus_{\mathbf{W}}$ -марковским.

Указаны такие разбиения $\mathbf{W} = \{\{\vec{0}_n\}, W_1, \dots, W_{r-1}\}$ пространства $V_n(2)$ с r блоками, $r \geq 3$, что существуют $\oplus_{\mathbf{W}}$ -марковские преобразования, принадлежащие группе изометрий $\text{Isom}(\mu)$ метрики $\mu: V_n(2) \times V_n(2) \rightarrow \{0, \dots, r-1\}$, инвариантной относительно группы сдвигов пространства $V_n(2)$ и однозначно задаваемой разбиением $\mathbf{W}$ посредством условия

$$\mu(\alpha, \alpha') = i, \quad \text{если} \quad \alpha \oplus \alpha' \in W_i, \quad i = 1, 2, \dots, r-1.$$

Прежде всего такие $\oplus_{\mathbf{W}}$ -марковские преобразования представляют интерес в связи с тем, что:

- 1) блоки разбиения $\mathbf{W}$ не равномощны, в частности они не являются смежными классами по некоторой подгруппе группы $(V_n(2), \oplus)$,
- 2) группа $\text{Isom}(\mu)$ может быть примитивной.

Заметим, что данные условия для преобразования $b \in \text{Isom}(\mu)$ означают отсутствие описанных в [3] «стандартных» гомоморфизмов алгоритма $C_l(\oplus, b)$, в некоторых случаях равносильных его $\oplus_{\mathbf{W}}$ -марковости.

2. Основные обозначения и понятия

В работе используются следующие обозначения:

- X — произвольное конечное непустое множество, $(X, \otimes)$ — произвольная абелева группа на множестве X с бинарной операцией $\otimes$ и единичным элементом e , $X^\times = X \setminus \{e\}$,
- $\alpha^b = \alpha b = b(\alpha)$ — образ элемента $\alpha \in X$ при действии на него подстановкой $b \in S(X)$, α^{-1} — обратный к α элемент относительно операции $\otimes$, $\alpha \bar{\otimes} \beta = \alpha \otimes \beta^{-1}$ для любых $\alpha, \beta \in X$,
- $I(A)$ — индикатор выполнения условия A ,
- K — множество всех раундовых ключей, $g: (\alpha, k) \mapsto g(\alpha, k)$ — раундовая функция, $g_k: \alpha \mapsto g(\alpha, k)$ — частичная раундовая функция, $(\alpha, k) \in X \times K$,
- $V_m = V_m(2)$ — векторное пространство размерности m над полем $GF(2)$,
- $P\{A\}$ — вероятность события A ,
- $\vec{1}_n$ — n -мерный вектор, каждая координата которого равна 1, $\vec{0}_n$ — нулевой n -мерный вектор,
- $\text{Aut}(\bar{\Gamma})$ — группа автоморфизмов графа (орграфа) $\bar{\Gamma}$,
- $B^b = \{\alpha^b \mid \alpha \in B\}$ для $B \subseteq X$, $b \in S(X)$, $\mathbf{W}^b = \{W_0^b, \dots, W_{r-1}^b\}$ для разбиения $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ множества X , $b \in S(X)$,
- $GL_n(R)$ ($AGL_n(R)$) — полная линейная (аффинная) группа над кольцом R , $GL_n = GL_n(GF(2))$, $AGL_n = AGL_n(GF(2))$,
- $V_n^+ (\mathbb{Z}_{2^n}^+)$ — регулярное подстановочное представление группы сдвигов пространства V_n (кольца $\mathbb{Z}_{2^n}$),
- $\langle b \rangle$ — циклическая группа, порожденная элементом $b \in S(X)$,
- $W^{\langle b \rangle} = \{\lambda^s \mid (\lambda, s) \in W \times \langle b \rangle\}$ для $W \subseteq X$, $b \in S(X)$.

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 $\zeta_{\mathbf{U}}^{(0)}, \zeta_{\mathbf{U}}^{(1)}, \dots$ со значениями в 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 ([6]). 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 $g: X^2 \mapsto X$ 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 $\xi^{(0)}$ на множестве X последовательность $\xi^{(t)} = (\xi^{(0)} \otimes \alpha)^{g_{k_1} \dots g_{k_t}} \otimes \alpha^{g_{k_1} \dots g_{k_t}}$, $t = 1, \dots, l$, 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.

Разбиения $\{X\}$, $\{\{\alpha\} \mid \alpha \in X\}$ множества X называются *тривиальными*.

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

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]). 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 $\hat{\mathbf{p}}_{\mathbf{W}}(b) = (\hat{p}_{W_j, W_c}(b))$ $\otimes_{\mathbf{W}}$ -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 $a_{j,c}$, $0 \leq a_{j,c} \leq 1$.

Очевидно, что преобразование и алгоритм блочного шифрования являются $\otimes_{\mathbf{W}}$ -марковскими, если разбиение $\mathbf{W}$ множества X тривиально или равно $\{\{e\}, X^{\times}\}$. Поэтому далее рассматриваются разбиения множества X , которые отличны от тривиального и $\{\{e\}, X^{\times}\}$.

Для разных криптографических приложений представляют интерес преобразования, которые не являются $\otimes_{\mathbf{W}}$ -марковскими для каждого нетривиального разбиения $\mathbf{W}$ множества X , $\mathbf{W} \neq \{\{e\}, X^{\times}\}$. Такие преобразования будем называть *абсолютно немарковскими*. Преобразования, которые не являются абсолютно немарковскими, будем называть *относительно марковскими*.

По определению каждое относительно марковское преобразование является $\otimes_{\mathbf{W}}$ -марковским для некоторого нетривиального разбиения $\mathbf{W}$ множества X , $\mathbf{W} \neq \{\{e\}, X^\times\}$. Вместе с тем для относительно марковского преобразования существует довольно много разбиений, для которых оно не является $\otimes_{\mathbf{W}}$ -марковским.

Рассмотрим декартово произведение

$$A \times B = \{(\alpha, \beta) \mid \alpha \in A, \beta \in B\}$$

двух конечных множеств A, B . Если $A \subseteq V_m, B \subseteq V_p$, то декартово произведение $A \times B$ будем рассматривать как подмножество пространства V_{m+p} , а пару $(\alpha, \beta) \in A \times B$, где

$$\alpha = (\alpha_{m-1}, \dots, \alpha_0), \quad \beta = (\beta_{p-1}, \dots, \beta_0),$$

отождествлять с $(m+p)$ -мерным вектором $(\alpha_{m-1}, \dots, \alpha_0, \beta_{p-1}, \dots, \beta_0)$. В данном контексте, если $n = d \cdot m, d > 1, d, m \in \mathbb{N}$, то векторное пространство V_n рассматривается и как декартово произведение V_m^d , а под разбиением декартова произведения V_m^d понимается разбиение пространства V_n .

Будем говорить, что преобразование $b \in S(X)$ *сохраняет (в целом) разбиение $\mathbf{W}$ множества X* , если $\mathbf{W}^b = \mathbf{W}$.

Определение 5. Пусть Y — произвольное конечное множество. Укрупнением разбиения $\mathbf{W} = \{W_0, \dots, W_{d-1}\}$ множества Y называется разбиение $\mathbf{W}' = \{W'_0, \dots, W'_{d'-1}\}$, 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 $\mathbf{W} \notin \{\{\alpha \mid \alpha \in X\}, \{X\}\}$.

3. Относительная марковость преобразований слоя S -боксов

Для произвольного $\oplus$ -марковского алгоритма блочного шифрования доказательство существования или отсутствия свойства $\oplus_{\mathbf{W}}$ -марковости в общем случае является сложной проблемой. Для XSL-алгоритмов блочного шифрования ($b = sh$) выявление $\oplus_{\mathbf{W}}$ -марковости подстановки b в ряде случаев может быть сведено к ее определению у компонент раундовой функции (нелинейного преобразования s слоя S -боксов и преобразования h линейного слоя). Так, рассмотрим XSL-алгоритм блочного шифрования с раундовой функцией

$g: V_n^2 \rightarrow V_n$, заданной условием

$$g: (\alpha, k) \mapsto (\alpha \oplus k)^{sh} \quad \text{для всех } (\alpha, k) \in V_n^2,$$

где $s = (s_{d-1}, \dots, s_0) \in S(V_m)^d$, $h \in GL_n$, $n = d \cdot m$, $d > 1$, причем

$$\beta^s = (\beta_{d-1}^{s_{d-1}}, \dots, \beta_0^{s_0}) \quad \text{для каждого } \beta = (\beta_{d-1}, \dots, \beta_0) \in V_m^d.$$

Пусть также $\mathbf{W}^{(j)}$ — такое разбиение пространства V_m на $r^{(j)}$ блоков, что S -блок s_j является $\oplus_{\mathbf{W}^{(j)}}$ -марковским для $j = 0, \dots, d-1$.

Для разбиений $\mathbf{W}^{(j)} = \{W_0^{(j)}, \dots, W_{r^{(j)}-1}^{(j)}\}$ пространства V_m ($j = 0, \dots, d-1$) положим

$$\begin{aligned} \overline{\mathbf{W}}_d &= \mathbf{W}^{(d-1)} \times \dots \times \mathbf{W}^{(0)} = \\ &= \{W_{i_{d-1}}^{(d-1)} \times W_{i_{d-2}}^{(d-2)} \times \dots \times W_{i_0}^{(0)} \mid (i_{d-1}, \dots, i_0) \in R^{(d)}\}, \end{aligned}$$

где $R^{(d)} = \{0, \dots, r^{(d-1)} - 1\} \times \dots \times \{0, \dots, r^{(0)} - 1\}$. Так как декартово произведение $W_{i_{d-1}}^{(d-1)} \times \dots \times W_{i_0}^{(0)} \in \overline{\mathbf{W}}_d$ рассматривается и как подмножество пространства V_n , то $\overline{\mathbf{W}}_d$ — разбиение V_n , каждый блок которого равен $W_{i_{d-1}}^{(d-1)} \times \dots \times W_{i_0}^{(0)}$ для некоторого $(i_{d-1}, \dots, i_0) \in R^{(d)}$.

Приведем достаточные условия на линейное преобразование h , из которых в случае $\oplus_{\mathbf{W}^{(j)}}$ -марковости каждого S -блока s_j для $j = 0, \dots, d-1$ будет вытекать $\oplus_{\overline{\mathbf{W}}_d}$ -марковость XSL-алгоритма блочного шифрования.

Утверждение 1. Пусть $d, m \in \mathbb{N}$, $n = d \cdot m$, $d > 1$, $s = (s_{d-1}, \dots, s_0) \in S(V_m)^d$, $h \in GL_n$ и частичная раундовая функция $g_k \in S(V_n)$ для каждого $k \in V_n$ задана условием

$$g_k: \alpha \mapsto (\alpha \oplus k)^{sh} \quad \text{для всех } \alpha \in V_n.$$

Пусть $\mathbf{W}^{(0)}, \dots, \mathbf{W}^{(d-1)}$ — такие разбиения пространства V_m на $r^{(j)}$ блоков, что подстановка s_j является $\oplus_{\mathbf{W}^{(j)}}$ -марковской для $j = 0, \dots, d-1$ и h сохраняет разбиение

$$\overline{\mathbf{W}}_d = \mathbf{W}^{(d-1)} \times \dots \times \mathbf{W}^{(0)}.$$

Тогда $\oplus$ -марковский алгоритм блочного шифрования с раундовой функцией g является $\oplus_{\overline{\mathbf{W}}_d}$ -марковским.

Доказательство. Очевидно, что для каждой пары $(\alpha, \varepsilon) \in V_n \times V_n^\times$ существует элемент $\delta_{\alpha, \varepsilon} \in V_n^\times$, удовлетворяющий равенству $(\alpha \oplus \varepsilon)^s = \alpha^s \oplus \delta_{\alpha, \varepsilon}$. Кроме того, из равенства

$$(\alpha \oplus \varepsilon)^{sh} = \alpha^{sh} \oplus (\delta_{\alpha, \varepsilon})^h$$

следует, что $\hat{p}_{\varepsilon, \delta}(s) = \hat{p}_{\varepsilon, \delta^h}(sh)$ для любых $\varepsilon, \delta \in V_n^\times$. Поэтому

$$\hat{p}_{\varepsilon, W}(s) = \hat{p}_{\varepsilon, W^h}(sh) = p_{\varepsilon, W^h}(g) \quad \text{для всех } \varepsilon \in V_n^\times, W \subset V_n. \quad (2)$$

Очевидно, что если $W^{(j)} \in \mathbf{W}^{(j)}$ для $j = 0, \dots, d-1$, то для каждого $\theta = (\theta_{d-1}, \dots, \theta_0) \in V_m^d$ справедливо равенство

$$\hat{p}_{\theta, W}(s) = \prod_{i=0}^{d-1} \hat{p}_{\theta_i, W^{(i)}}(s_i) \quad \text{для } W = W^{(d-1)} \times \dots \times W^{(0)}. \quad (3)$$

Так как s_j — $\oplus_{\mathbf{W}^{(j)}}$ -марковская подстановка для каждого $j \in \{0, \dots, d-1\}$, то из равенства (3) следует $\oplus_{\overline{\mathbf{W}}_d}$ -марковость подстановки $s = (s_{d-1}, \dots, s_0)$. Таким образом, из условия сохранения разбиения $\overline{\mathbf{W}}_d$ преобразованием h , равенства (2) и $\oplus_{\overline{\mathbf{W}}_d}$ -марковости подстановки s вытекает $\oplus_{\overline{\mathbf{W}}_d}$ -марковость алгоритма блочного шифрования с раундовой функцией g . $\square$

Согласно утверждению 1 из $\oplus_{\mathbf{W}^{(j)}}$ -марковости S -блока s_j ($j=0, \dots, d-1$) и того, что линейное преобразование h сохраняет разбиение $\overline{\mathbf{W}}_d$, вытекает $\oplus_{\overline{\mathbf{W}}_d}$ -марковость XSL-алгоритма блочного шифрования. Очевидно, что если преобразование $h \in AGL_n$ сохраняет некоторое разбиение $\overline{\mathbf{W}}_d$ пространства V_n , то h — $\oplus_{\overline{\mathbf{W}}}$ -марковское преобразование. В связи с этим в данном разделе рассматриваются условия выполнения свойства $\oplus_{\mathbf{W}}$ -марковости у S -блоков, а в разделе 4 они описываются для преобразования h линейного слоя.

В последние годы в криптографической литературе (см., например, [7–12]) большое внимание уделяется связям аффинно-эквивалентных S -блоков. Поэтому естественно рассмотреть влияние аффинной эквивалентности на свойство $\oplus_{\mathbf{W}}$ -марковости S -блоков.

Определение 7. Подстановки $s, s' \in S(V_n)$ называются аффинно-эквивалентными, если существуют такие $h^{(1)}, h^{(2)} \in AGL_n$, что $s' = h^{(1)}sh^{(2)}$.

Рассмотрим аффинно-эквивалентные подстановки $s, s' \in S(V_n)$ и укажем достаточные условия на разбиения $\mathbf{W}, \mathbf{W}'$ пространства V_n , при выполнении которых s, s' являются соответственно $\oplus_{\mathbf{W}}$ - и $\oplus_{\mathbf{W}'}$ -марковскими. Для $\oplus_{\mathbf{W}}$ -марковской подстановки $s \in S(V_n)$ приведем условия, из которых вытекает $\oplus_{\mathbf{W}'}$ -марковость аффинно-эквивалентных подстановок для некоторого разбиения $\mathbf{W}'$.

Для разбиения $\mathbf{W}$ пространства V_n и подгруппы $G \leq S(V_n)$ положим $G_{\mathbf{W}} = \{g \in G \mid \mathbf{W}^g = \mathbf{W}\}$.

Аффинное преобразование $h \in AGL_n$ иногда будет удобно записывать в виде пары $(h_0, \delta) \in GL_n \times V_n$, заданной условием $h: \alpha \mapsto \alpha^{h_0} \oplus \delta$.

Утверждение 2. Пусть $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ — нетривиальное разбиение пространства V_n , s — произвольная $\oplus_{\mathbf{W}}$ -марковская подстановка из $S(V_n)$. Тогда для любых аффинных преобразований $a = (a_0, \delta)$, $b = (b_0, \delta')$ из AGL_n , удовлетворяющих включению $b_0 a_0 \in GL_{\mathbf{W}}$, подстановка $s' = a s b$ является $\oplus_{\mathbf{W}^{b_0}}$ -марковской для разбиения $\mathbf{W}^{b_0}$ пространства V_n .

Доказательство. Из определения 4 следует, что

$$\hat{p}_{\theta, W_c}(s) = \sum_{\theta' \in W_c} \hat{p}_{\theta, \theta'}(s) = \sum_{\theta' \in W_c} \hat{p}_{\delta, \theta'}(s) \quad (4)$$

для всех $\theta, \delta \in W_i$, $i, c \in \{0, \dots, r-1\}$. Очевидно, что

$$\hat{p}_{\varepsilon, \lambda}(s') = \hat{p}_{\varepsilon a_0, \lambda b_0^{-1}}(s) \text{ для любых } \varepsilon, \lambda \in V_n. \quad (5)$$

Из равенств (4), (5) вытекает, что

$$\hat{p}_{\theta, W_c}(s) = \hat{p}_{\theta', W_c}(s) = \hat{p}_{\theta a_0^{-1}, W_c^{b_0}}(s') = \hat{p}_{(\theta') a_0^{-1}, W_c^{b_0}}(s')$$

для всех $\theta, \theta' \in W_i$, $i, c \in \{0, \dots, r-1\}$, т. е.

$$\hat{p}_{\theta a_0^{-1}, W_c^{b_0}}(s') = \hat{p}_{\theta' a_0^{-1}, W_c^{b_0}}(s').$$

Отсюда для всех $\lambda, \lambda' \in W_i^{a_0^{-1}}$, $i, c \in \{0, \dots, r-1\}$ следует равенство

$$\hat{p}_{\lambda, W_c^{b_0}}(s') = \hat{p}_{\lambda', W_c^{b_0}}(s'). \quad (6)$$

Таким образом, если $\mathbf{W}^{a_0^{-1}} = \mathbf{W}^{b_0}$, то $W_i^{a_0^{-1}}, W_i^{b_0} \in \mathbf{W}^{b_0}$ для каждого $i \in \{0, \dots, r-1\}$, а $b_0 a_0 \in GL_{\mathbf{W}}$. Поэтому из равенства (6) вытекает, что $\hat{p}_{\lambda, W_c^{b_0}}(s') = \hat{p}_{\lambda', W_c^{b_0}}(s')$ для всех $\lambda, \lambda' \in W_i^{b_0}$, $i, c \in \{0, \dots, r-1\}$, т. е. s' — $\oplus_{\mathbf{W}^{b_0}}$ -марковская подстановка согласно определению 4. $\square$

Таким образом, в утверждении 2 для произвольной $\oplus_{\mathbf{W}}$ -марковской подстановки s описано семейство аффинно-эквивалентных относительно марковских подстановок.

Каждой подстановке $b \in S(V_n)$ поставим в соответствие (взвешенный) орграф (с петлями) $\bar{\Gamma}(b)$ с множеством вершин $V_n^\times$ и множеством дуг $\Delta^{(s)}$,

определяемым $(2^n-1) \times (2^n-1)$ -матрицей смежности $\mathbf{q}(b) = (q_{i,j}(b))$, где при $i, j \in \{1, \dots, 2^n-1\}$ элемент $q_{i,j}(b)$ задается условием

$$q_{i,j}(b) = \begin{cases} 1, & \text{если } \hat{p}_{i,j}(b) \neq 0, \\ 0, & \text{если } \hat{p}_{i,j}(b) = 0, \end{cases}$$

при этом дуга (i, j) имеет вес $\hat{p}_{i,j}(b)$, если $\hat{p}_{i,j}(b) \neq 0$.

Группа автоморфизмов $\text{Aut}(\bar{\Gamma}(b))$ взвешенного орграфа $\bar{\Gamma}(b)$ с множеством вершин $V_n^\times$ задается условием

$$\text{Aut}(\bar{\Gamma}(b)) = \{g \in S(V_n^\times) \mid \hat{p}_{i,j}(b) = \hat{p}_{ig,jg}(b) \ \forall (i, j) \in (V_n^\times)^2\}.$$

Утверждение 3. Пусть b — произвольная подстановка на V_n . Тогда для каждого элемента

$$g = (\alpha_1^{(1)}, \dots, \alpha_{d_1}^{(1)}) \dots (\alpha_1^{(r)}, \dots, \alpha_{d_r}^{(r)}) \in \text{Aut}(\bar{\Gamma}(b))$$

она является $\oplus_{\mathbf{W}^{(g)}}$ -марковской для разбиения $\mathbf{W}^{(g)} = \{W_0, \dots, W_r\}$, где

$$W_0 = \{\vec{0}_n\}, \quad W_j = \{\alpha_1^{(j)}, \dots, \alpha_{d_j}^{(j)}\} \quad \text{при } j = 1, \dots, r.$$

Кроме того, если подстановка g не является тождественной или полноцикловой, то разбиение $\mathbf{W}^{(g)}$ нетривиально и отлично от $\{\{\vec{0}_n\}, V_n^\times\}$.

Доказательство. Заметим, что для всех $\theta \in W_i$, $i, j \in \{0, \dots, r\}$, справедливо равенство

$$\sum_{\theta' \in W_j} \hat{p}_{\theta, \theta'}(b) = \hat{p}_{\theta, W_j}(b) \quad (7)$$

и $\sum_{\theta' \in W_j} \hat{p}_{\theta, \theta'}(b)$ — сумма весов всех дуг, исходящих из вершины θ в вершины, принадлежащие множеству W_j . Так как $g \in \text{Aut}(\bar{\Gamma}(b))$, то для каждого $c \in \{1, \dots, d_i\}$ сумма весов всех дуг, исходящих из вершины θ^{g^c} в вершины, принадлежащие множеству W_j , равна одному и тому же рациональному числу $a_{i,j}(b)$. Таким образом, из равенства (7) вытекает, что

$$\hat{p}_{\theta, W_j}(b) = a_{i,j}(b) \quad \text{для всех } \theta \in W_i, \quad i, j \in \{0, \dots, r\}.$$

Из утверждения 3 [2] следует $\oplus_{\mathbf{W}^{(g)}}$ -марковость подстановки b .

Заметим, что если $g = e$, то разбиение $\mathbf{W}^{(g)}$ тривиально. Кроме того, полноцикловой подстановке g соответствует разбиение

$$\mathbf{W}^{(g)} = \{\{\vec{0}_n\}, V_n^\times\}. \quad \square$$

Криптографический интерес представляют $\oplus_{\mathbf{W}}$ -марковские преобразования только для нетривиального разбиения $\mathbf{W}$ пространства V_n , $\mathbf{W} \neq \{\{\vec{0}_n\}, V_n^\times\}$. Если $\text{Aut}(\bar{\Gamma}(b)) = \{e\}$, то из утверждения 3 следует только $\oplus_{\mathbf{W}}$ -марковость для тривиального разбиения $\mathbf{W}$. Покажем далее, что $\oplus_{\mathbf{W}}$ -марковская подстановка b существует для нетривиального разбиения $\mathbf{W}$ даже при равенстве $\text{Aut}(\bar{\Gamma}(b)) = \{e\}$.

Следствие 1. Пусть b — произвольная подстановка на V_n и существует такое подмножество $W \subseteq V_n^\times$, что

$$\hat{p}_{\theta, W}(b) = \hat{p}_{\theta', W}(b) \quad \text{для всех} \quad (\theta, \theta') \in W^2 \cup (V_n^\times \setminus W)^2.$$

Тогда:

- 1) подстановка b — $\oplus_{\mathbf{W}}$ -марковская для разбиения $\mathbf{W} = \{\{\vec{0}_n\}, W, V_n^\times \setminus W\}$;
- 2) если $\bar{\Gamma}_W(b)$ — (взвешенный) подорграф орграфа $\bar{\Gamma}(b)$ с множеством вершин $W \subseteq V_n^\times$, то для каждого элемента

$$g = (\alpha_1^{(1)}, \dots, \alpha_{d_1}^{(1)}) \dots (\alpha_1^{(r)}, \dots, \alpha_{d_r}^{(r)}) \in \text{Aut}(\bar{\Gamma}_W(b))$$

подстановка b является $\oplus_{\mathbf{W}^{(g)}}$ -марковской для разбиения

$$\mathbf{W}^{(g)} = \{\{\vec{0}_n\}, W_1^{(g)}, \dots, W_r^{(g)}, V_n^\times \setminus W\},$$

$$\text{где } W_j^{(g)} = \{\alpha_1^{(j)}, \dots, \alpha_{d_j}^{(j)}\} \text{ для } j = 1, \dots, r \text{ и } W = \bigcup_{j=1}^r W_j^{(g)}.$$

Доказательство следует из определения 4 и утверждения 3. $\square$

Заметим, что если в условии следствия 1 подмножество $W \subseteq V_n^\times$ таково, что $\text{Aut}(\bar{\Gamma}_W(b)) = \{e\}$, то совпадают разбиения $\mathbf{W}$, $\mathbf{W}^{(e)}$, заданные соответственно в п. 1 и п. 2. Кроме того, если существует полноцикловая подстановка $g \in \text{Aut}(\bar{\Gamma}_W(b))$, $\text{Aut}(\bar{\Gamma}_W(b)) \neq \{e\}$, то $\mathbf{W}' = \mathbf{W}^{(g)}$. Поэтому в п. 2 с точки зрения описания нетривиального разбиения $\mathbf{U}$, относительно которого подстановка b является $\oplus_{\mathbf{U}}$ -марковской, представляют интерес условия существования неполноцикловой подстановки $g \in \text{Aut}(\bar{\Gamma}_W(b)) \setminus \{e\}$.

Из п. 1 следствия 1 вытекает, что для нахождения разбиения $\mathbf{W}$ множества $V_n^\times$, относительно которого подстановка $b \in S(V_n)$ является $\oplus_{\mathbf{W}}$ -марковской, достаточно найти подмножество $W \subseteq V_n^\times$, удовлетворяющее условию $\hat{p}_{\theta, W}(b) = \hat{p}_{\theta', W}(b)$ для всех $(\theta, \theta') \in W^2 \cup (V_n^\times \setminus W)^2$. Для этого, вместо последовательного перебора всех подмножеств множества $V_n^\times$ мощностей

$2, 3, \dots, n-1$, можно искать такой подорграф $\bar{\Gamma}_W(b)$ с множеством вершин W орграфа $\bar{\Gamma}(b)$, что группе $\text{Aut}(\bar{\Gamma}_W(b))$ принадлежит подстановка, орбитой которой является множество W .

В криптографических приложениях активно используются APN-преобразования, введенные в [13]. Преобразование $b: V_n \rightarrow V_n$ называется APN (almost perfect nonlinear), если

$$\max \{ \widehat{p}_{\varepsilon, \delta}(b) \mid (\varepsilon, \delta) \in V_n^\times \times V_n \} = 2^{1-n}.$$

Обобщением APN-преобразований являются разностно d -равномерные отображения (differentially d -uniform). В работе будем следовать определению 8 (см., например, [14–17]).

Определение 8. Для числа $d \in \mathbb{N}$ преобразование $b: V_n \rightarrow V_n$ называется разностно d -равномерным, если

$$\max \{ \widehat{p}_{\varepsilon, \delta}(b) \mid (\varepsilon, \delta) \in V_n^\times \times V_n \} = 2^{-n}d.$$

Разностно 2-равномерное преобразование называется также APN-преобразованием.

Рассмотрим применение утверждения 3 и следствия 1 к APN-подстановкам и разностно 4-равномерным подстановкам. Сначала для APN-подстановки $s \in S(V_n)$ укажем такой способ выбора разбиения $\mathbf{W}$ пространства V_n , что s — $\oplus_{\mathbf{W}}$ -марковская. Кроме того, опишем такую аффинно-эквивалентную подстановке s подстановку s' и такое разбиение $\mathbf{W}'$ пространства V_n , что s' — $\oplus_{\mathbf{W}'}$ -марковская, а также укажем связь между разбиениями $\mathbf{W}$, $\mathbf{W}'$.

Пример 1. Пусть s — произвольная APN-подстановка из $S(V_n)$, а $s' = asb$ для аффинных преобразований $a = (a_0, \delta)$, $b = (b_0, \delta')$ из AGL_n , где $a_0^{-1} = b_0$. Тогда из равенства (5) следует, что для каждой подстановки $g \in \text{Aut}(\bar{\Gamma}(s))$ справедливо включение $a_0 g a_0^{-1} \in \text{Aut}(\bar{\Gamma}(s'))$.

Согласно утверждению 9 [2], если

$$g = (\alpha_1^{(1)}, \dots, \alpha_{d_1}^{(1)}) \dots (\alpha_1^{(r)}, \dots, \alpha_{d_r}^{(r)}),$$

то s — $\oplus_{\mathbf{W}(g)}$ -марковская подстановка, а потому s' — $\oplus_{\mathbf{W}'(g)}$ -марковская подстановка, где

$$\begin{aligned} \mathbf{W}^{(g)} &= \{W_0, \dots, W_r\}, \quad \mathbf{W}'^{(g)} = \{W'_0, \dots, W'_r\}, \\ W_0 &= W'_0 = \{\vec{0}_n\}, \quad W_i = \{\alpha_1^{(i)}, \dots, \alpha_{d_i}^{(i)}\}, \quad W'_i = W_i^{b_0}, \quad i = 1, \dots, r. \end{aligned}$$

Очевидно, что если оргграфы $\bar{\Gamma}(s)$, $\bar{\Gamma}(s')$ изоморфны, то $a_0 \in \text{Aut}(\bar{\Gamma}(s))$. Таким образом, если APN-подстановка s такова, что разбиение $\mathbf{W}^{(g)}$ нетривиально для некоторой нетождественной подстановки $g \in \text{Aut}(\bar{\Gamma}(s))$, то для каждого линейного преобразования $a_0 \in GL_n$ существует $\oplus_{\widetilde{\mathbf{W}}^{(a,g)}}$ -марковская подстановка, аффинно эквивалентная s , где $\widetilde{\mathbf{W}}^{(a,g)} = (\mathbf{W}^{(g)})^{a^{-1}}$.

Пример 2. Пусть $m = 3$, $GF(2^3) = GF(2)[x]/(x^3 \oplus x \oplus 1)$. Элементы поля $GF(2^3)$ естественным образом будем отождествлять с элементами множества $\{0, 1, \dots, 7\}$.

Рассмотрим APN-подстановку $s \in S(GF(2^3))$, заданную условием

$$s: \alpha \mapsto \begin{cases} \alpha^{-1}, & \text{если } \alpha \neq 0, \\ 0, & \text{если } \alpha = 0. \end{cases}$$

Нетрудно убедиться, что $\bar{\Gamma}(s) = (\{1, \dots, 7\}, \Delta^{(s)})$ — оргграф с множеством дуг

$$\begin{aligned} \Delta^{(s)} = \{ & (1, 1), (2, 2), (4, 4), (6, 6), (1, 3), (3, 1), \\ & (1, 5), (5, 1), (1, 7), (7, 1), (6, 7), (7, 6), (2, 3), (3, 2), \\ & (2, 6), (2, 7), (3, 5), (3, 6), (4, 2), (4, 3), (4, 5), \\ & (5, 2), (5, 4), (5, 7), (6, 4), (6, 5), (7, 3), (7, 4) \} \end{aligned}$$

и группой автоморфизмов

$$\text{Aut}(\bar{\Gamma}(s)) = \{e, (4,6)(5,7), (2,4)(3,5), (2,6)(3,7), (2,4,6)(3,5,7), (2,6,4)(3,7,5)\}.$$

Полный перебор всех линейных преобразований $a_0, b_0 \in GL_3$ показал, что для каждой пары $a = (a_0, \delta)$, $b = (b_0, \delta')$ из AGL_3 преобразование $s' = asb$ обладает следующими свойствами:

- 1) $|\text{Aut}(\bar{\Gamma}(s'))| \in \{2, 3, 4, 6\}$,
- 2) s' — $\oplus_{\mathbf{W}'}$ -марковская для нетривиального разбиения $\mathbf{W}'$, у которого число и мощности блоков удовлетворяют одному из условий:
 - 2 блока мощности 2, 4 блока мощности 1,
 - 2 блока мощности 3, 2 блока мощности 1,
 - 3 блока мощности 2, 2 блока мощности 1.

Используя утверждение 3, укажем такие разбиения $\mathbf{W}$ пространства V_4 , что разностно 4-равномерные подстановки из $S(V_4)$ являются $\oplus \mathbf{W}$ -марковскими.

Пример 3. Пусть $m = 4$, $GF(2^4) = GF(2)[x]/(x^4 \oplus x \oplus 1)$. Элементы поля $GF(2^4)$ естественным образом будем отождествлять с элементами множества $\{0, 1, \dots, 15\}$, а также с векторами из пространства V_4 .

Рассмотрим разностно 4-равномерную подстановку $s \in S(GF(2^4))$, заданную условием

$$s: \alpha \mapsto \begin{cases} \alpha^{-1}, & \text{если } \alpha \neq 0, \\ 0, & \text{если } \alpha = 0. \end{cases}$$

Непосредственными вычислениями находится матрица $\hat{\mathbf{p}}(s)$, однозначно задающая множество дуг $\Delta^{(s)}$ и весов взвешенного орграфа

$$\bar{\Gamma}(s) = (\{1, \dots, 15\}, \Delta^{(s)}).$$

Матрица $\hat{\mathbf{p}}(s)$ такова, что $\mathbf{q}(s)$ – симметричная матрица, $\bar{\Gamma}(s)$ – граф, а

$$\hat{p}_{\theta, \theta'}(s) = 2^{-2} \quad \text{для всех } \{\theta, \theta'\} \in \Theta,$$

где

$$\Theta = \{\{1\}, \{2, 9\}, \{3, 14\}, \{5, 11\}, \{6, 7\}, \{8, 15\}, \{10, 12\}, \{4, 13\}\}.$$

Ясно, что каждая подстановка $g \in \text{Aut}(\bar{\Gamma}(s))$ удовлетворяет условию $\Theta^g = \Theta$, т.е. $g: 1 \mapsto 1$ и $\Theta'^g = \Theta'$, где $\Theta' = \Theta \setminus \{1\}$. Эти условия существенно облегчают нахождение элементов группы $\text{Aut}(\bar{\Gamma}(s))$. Нетрудно убедиться, что $|\text{Aut}(\bar{\Gamma}(s))| \leq 7! 2^7 \leq 2^{19,3}$.

Непосредственными вычислениями показывается, что разбиением $\mathbf{W}$ множества $\{0, 1, \dots, 15\}$, при котором подстановка s является $\oplus \mathbf{W}$ -марковской, служит $\{W_0, \dots, W_6\}$, где

$$W_0 = \{0\}, W_1 = \{1\}, W_2 = \{2, 3, 4, 5\}, W_3 = \{9, 14, 13, 11\},$$

$$W_4 = \{6, 7\}, W_5 = \{10, 12\}, W_6 = \{8, 15\},$$

$$\hat{\mathbf{p}}_{\mathbf{W}}(s) = 2^{-4} \begin{pmatrix} 16 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 8 & 4 & 0 & 0 \\ 0 & 0 & 2 & 6 & 2 & 4 & 2 \\ 0 & 2 & 6 & 4 & 0 & 2 & 2 \\ 0 & 2 & 4 & 0 & 6 & 4 & 0 \\ 0 & 0 & 6 & 4 & 2 & 4 & 0 \\ 0 & 0 & 6 & 4 & 2 & 0 & 4 \end{pmatrix}.$$

Пусть теперь некоторая разностно 4-равномерная подстановка $s \in S(V_4)$ удовлетворяет следующему условию: для каждого $\theta \in V_4^\times$ существует такой единственный $\theta' \in V_4^\times$, что $\hat{p}_{\theta, \theta'}(s) = 2^{-2}$. Очевидно, что для некоторой подстановки $u_s: V_4^\times \rightarrow V_4^\times$ выполняется равенство $\hat{p}_{\theta, \theta u_s}(s) = 2^{-2}$ для каждого $\theta \in V_4^\times$. В этом случае для поиска разбиения $\mathbf{W}$, относительно которого s является $\oplus \mathbf{W}$ -марковской, можно рассматривать компоненты связности орграфа $\bar{\Gamma}(u_s)$ и преобразования, сохраняющие «в целом» его компоненты связности или некоторые объединения компонент связности. Далее приведем соответствующие примеры 4 – 6.

Пример 4. Пусть $m = 4$, $GF(2^4) = GF(2)[x]/(x^4 \oplus x \oplus 1)$. Элементы поля $GF(2^4)$ естественным образом будем отождествлять с элементами множества $\{0, 1, \dots, 15\}$, а также с векторами из пространства V_4 .

Рассмотрим разностно 4-равномерную подстановку $s \in S(GF(2^4))$, заданную условием

$$s: \alpha \mapsto \begin{cases} \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \alpha^{-1}, & \text{если } \alpha \neq \vec{0}_4, \\ \vec{0}_4, & \text{если } \alpha = \vec{0}_4. \end{cases}$$

Заметим, что вектор $\vec{0}_4$ отождествляется с нулевым элементом поля $GF(2^4)$, а также с элементом 0 множества $\{0, 1, \dots, 15\}$.

Непосредственными вычислениями находится матрица $\hat{\mathbf{p}}(s)$, однозначно задающая множество дуг $\Delta^{(s)}$ и весов взвешенного орграфа $\bar{\Gamma}(s) = (\{1, \dots, 15\}, \Delta^{(s)})$. Матрица $\hat{\mathbf{p}}(s)$ такова, что $\hat{p}_{\theta, \theta'}(s) = 2^{-2}$ для всех $(\theta, \theta') \in \Theta$, где

$$\Theta = \{(1,7), (2,9), (3,8), (4,4), (5,2), (6,1), (7,6), (8,15), (9,11), \\ (10,3), (11,10), (12,5), (13,13), (14,12), (15,14)\}.$$

Несложно убедиться, что $\text{Aut}(\bar{\Gamma}(s)) = \{e\}$. Зададим преобразование $u_s: \{1, 2, \dots, 15\} \rightarrow \{1, 2, \dots, 15\}$ условием $u_s: \theta \mapsto \varepsilon$ тогда и только тогда, когда $\hat{p}_{\theta, \varepsilon}(s) = 2^{-2}$ для $\theta, \varepsilon \in \{1, \dots, 15\}$. Орграф $\bar{\Gamma}(u_s) = (\{1, 2, \dots, 15\}, \Theta)$ преобразования u_s состоит из 4 компонент связности:

$$\begin{aligned} \bar{\Gamma}^{(1)}(u_s) &= (\{4\}, \{(4,4)\}), \quad \bar{\Gamma}^{(2)}(u_s) = (\{13\}, \{(13,13)\}), \\ \bar{\Gamma}^{(3)}(u_s) &= (\{1,6,7\}, \{(1,7), (7,6), (6,1)\}), \\ \bar{\Gamma}^{(4)}(u_s) &= (\{1,2,\dots,15\} \setminus \{1,6,7,4,13\}, \{(2,9), (3,8), (5,2), (8,15), (9,11), (10,3), \\ &\quad (11,10), (12,5), (14,12), (15,14)\}). \end{aligned}$$

Нетрудно проверить, что множество $W = \{1, 6, 7\}$ вершин компоненты $\bar{\Gamma}^{(3)}(u_s)$ удовлетворяет следующим условиям:

- $\hat{p}_{\theta, W}(s) = \hat{p}_{\theta', W}(s)$ для всех $(\theta, \theta') \in W^2 \cup (\{1, 2, \dots, 15\} \setminus W)^2$,
- $(1, 6, 7) \in \text{Aut}(\bar{\Gamma}_W(s))$.

Из утверждения 3 следует, что s — $\oplus \mathbf{W}$ -марковская подстановка относительно разбиения $\mathbf{W} = \{W_0, W_1, W_2\}$, где

$$W_0 = \{0\}, \quad W_1 = \{1, 6, 7\}, \quad W_2 = \{1, 2, \dots, 15\} \setminus W_1.$$

Пример 5. Пусть $m = 4$, $GF(2^4) = GF(2)[x]/(x^4 \oplus x \oplus 1)$. Элементы поля $GF(2^4)$ естественным образом будем отождествлять с элементами множества $\{0, 1, \dots, 15\}$, а также с векторами из пространства V_4 .

Рассмотрим разностно 4-равномерную подстановку $s \in S(GF(2^4))$, заданную условием $s = (1, 7, 4, 13)(2, 14, 8, 11)(3, 9, 12, 6)$.

Непосредственными вычислениями находится матрица $\hat{\mathbf{p}}(s)$, однозначно задающая множество дуг $\Delta^{(s)}$ и весов взвешенного орграфа $\bar{\Gamma}(s) = (\{1, \dots, 15\}, \Delta^{(s)})$. Матрица $\hat{\mathbf{p}}(s)$ такова, что $\hat{p}_{\theta, \theta'}(s) = 2^{-2}$ для всех $(\theta, \theta') \in \Theta$, где

$$\Theta = \{(1, 7), (2, 12), (3, 8), (4, 1), (5, 2), (6, 4), (7, 3), (8, 15), \\ (9, 14), (10, 6), (11, 10), (12, 5), (13, 13), (14, 9), (15, 11)\}.$$

Нетрудно убедиться, что $\text{Aut}(\bar{\Gamma}(s)) = \{e\}$. Зададим преобразование $u_s: \{1, 2, \dots, 15\} \rightarrow \{1, 2, \dots, 15\}$ условием $u_s: \theta \mapsto \varepsilon$ тогда и только тогда, когда $\hat{p}_{\theta, \varepsilon}(s) = 2^{-2}$. Орграф $\bar{\Gamma}(u_s) = (\{1, 2, \dots, 15\}, \Theta)$ преобразования u_s состоит из трех компонент связности:

$$\begin{aligned} \bar{\Gamma}^{(1)}(u_s) &= (\{13\}, \{(13, 13)\}), \\ \bar{\Gamma}^{(2)}(u_s) &= (\{12, 5, 2\}, \{(12, 5), (5, 2), (2, 12)\}), \\ \bar{\Gamma}^{(3)}(u_s) &= (\{1, \dots, 15\} \setminus \{13, 2, 12, 5\}, \{(1, 7), (3, 8), (4, 1), (6, 4), (7, 3), (8, 15), \\ &\quad (9, 14), (10, 6), (11, 10), (14, 9), (15, 11)\}). \end{aligned}$$

Заметим, что множество вершин W ни для одной из компонент связности $\bar{\Gamma}^{(1)}(u_s)$, $\bar{\Gamma}^{(2)}(u_s)$, $\bar{\Gamma}^{(3)}(u_s)$ не удовлетворяет условию $\hat{p}_{\theta, W}(s) = \hat{p}_{\theta', W}(s)$ для всех $(\theta, \theta') \in W^2 \cup (\{1, \dots, 15\} \setminus W)^2$. Кроме того,

- $\text{Aut}(\bar{\Gamma}_W(s)) = \langle (5, 2) \rangle$, если $W = \{12, 5, 2\}$,

- $\text{Aut}(\bar{\Gamma}_W(s)) = \{e\}$, если $W = \{1, \dots, 15\} \setminus \{13, 2, 12, 5\}$.

Перебором всех возможных нетривиальных разбиений множества $\{1, \dots, 15\}$ можно показать, что s является абсолютно немарковской подстановкой.

Пример 6. Пусть $m = 4$, $GF(2^4) = GF(2)[x]/(x^4 \oplus x^3 \oplus 1)$. Элементы поля $GF(2^4)$ естественным образом будем отождествлять с элементами множества $\{0, 1, \dots, 15\}$, а также с векторами из пространства V_4 .

Рассмотрим разностно 4-равномерную подстановку $s \in S(GF(2^4))$, заданную условием

$$s: \alpha \mapsto \begin{cases} \alpha^{-1}, & \text{если } \alpha \neq 0, \\ 0, & \text{если } \alpha = 0. \end{cases}$$

Непосредственными вычислениями находится матрица $\hat{\mathbf{p}}(s)$, однозначно задающая множество дуг $\Delta^{(s)}$ и весов взвешенного орграфа $\bar{\Gamma}(s) = (\{1, \dots, 15\}, \Delta^{(s)})$. Матрица $\hat{\mathbf{p}}(s)$ такова, что $\mathbf{q}(s)$ — симметричная матрица, а $\hat{p}_{\theta, \theta'}(s) = \hat{p}_{\theta', \theta}(s) = 2^{-2}$ для всех $(\theta, \theta') \in \Theta$, где

$$\Theta = \{(1,7), (2,12), (3,8), (4,1), (5,2), (6,4), (7,3), (8,15), \\ (9,14), (10,6), (11,10), (12,5), (13,13), (14,9), (15,11)\}.$$

Снова каждая подстановка $g \in \text{Aut}(\bar{\Gamma}(s))$ удовлетворяет условию $\Theta^g = \Theta$, т.е. $g: 1 \mapsto 1$ и $\Theta'^g = \Theta'$, где $\Theta' = \Theta \setminus \{1\}$. Непосредственными вычислениями показывается, что разбиение $\mathbf{W}$ множества $\{0, \dots, 15\}$, при котором подстановка s является $\oplus_{\mathbf{W}}$ -марковской, — это разбиение $\{W_0, \dots, W_5\}$, в котором

$$W_0 = \{0\}, \quad W_1 = \{1\}, \quad W_2 = \{10, 11\}, \quad W_3 = \{2, 4, 9, 14\},$$

$$W_4 = \{3, 5, 8, 15\}, \quad W_5 = \{6, 7, 12, 13\}.$$

В примерах 1–6 указаны $\oplus_{\mathbf{W}}$ -марковские подстановки для таких разбиений $\mathbf{W}$ пространства V_m ($m \in \{3, 4\}$), что блоки $\mathbf{W}$ не являются: 1) равномошными, 2) объединением смежных классов по некоторому подпространству V_m .

Тем самым показано, что из условия $\oplus_{\mathbf{W}}$ -марковости подстановки не всегда вытекает ее принадлежность некоторой импримитивной группе подстановок. Поэтому для указанных выше подстановок не существует описанного в [3] «стандартного» гомоморфизма.

4. Относительная марковость преобразования линейного слоя

В утверждении 1 приведены достаточные условия $\oplus_{\mathbf{W}}$ -марковости раундовой функции, вытекающие из $\oplus_{\mathbf{W}}$ -марковости слоя S -боксов и свойств линейного преобразования h раундовой функции XSL-алгоритма. В разделе 3 (см. утверждение 3, следствие 1) описаны достаточные условия $\oplus_{\mathbf{W}}$ -марковости слоя S -боксов.

В этом разделе в связи с выявлением $\oplus_{\mathbf{W}}$ -марковости преобразования линейного слоя для произвольного аффинного преобразования $h \in AGL_n$ будет приведено описание нетривиальных разбиений $\mathbf{W}$ пространства V_n , $\mathbf{W} \neq \{\{\vec{0}_n\}, V_n^\times\}$, относительно которых h является $\oplus_{\mathbf{W}}$ -марковским. Оно основано на свойствах орграфа $\bar{\Gamma}(b) = (V_n^\times, \{(\alpha, \alpha^b) | \alpha \in V_n^\times\})$ линейного преобразования $b \in GL_n$. В частности, будет получен критерий абсолютной немарковости аффинных преобразований из AGL_n .

Далее орграф $\bar{\Gamma}(b)$, следуя принятой традиции (см., например, [19, 20]), будем называть графом преобразования.

Утверждение 4. Пусть $n \geq 2$, (b, δ) — произвольное аффинное преобразование на V_n , заданное условием $(b, \delta): \alpha \mapsto \alpha^b \oplus \delta$, $b \in GL_n$, $\delta \in V_n$, а граф $\bar{\Gamma}(b) = (V_n^\times, \{(\alpha, \alpha^b) | \alpha \in V_n^\times\})$ преобразования b состоит из d компонент связности $\bar{\Gamma}_1(b), \dots, \bar{\Gamma}_d(b)$ соответственно с множеством вершин $B_1, \dots, B_d$. Пусть также для каждого $i \in \{1, \dots, d\}$ подстановка $g_i \in \text{Aut}(\bar{\Gamma}_i(b))$ произвольна, а циклическая группа $\langle g_i \rangle$ имеет t_i орбит $W_i^{(1)}, \dots, W_i^{(t_i)}$. Тогда (b, δ) является $\oplus_{\mathbf{W}}$ -марковским преобразованием для разбиения

$$\mathbf{W} = \{\{\vec{0}_n\}\} \cup \bigcup_{i=1}^d \{W_i^{(1)}, \dots, W_i^{(t_i)}\}.$$

Кроме того, если $\mathbf{T}$ — произвольное разбиение множества $\{1, \dots, d\}$, то (b, δ) является $\oplus_{\mathbf{W}_{\mathbf{T}}}$ -марковским преобразованием для разбиения

$$\mathbf{W}_{\mathbf{T}} = \{\{\vec{0}_n\}\} \cup \bigcup_{T \in \mathbf{T}} \{\tilde{B}_T\}, \quad \text{где} \quad \tilde{B}_T = \bigcup_{j \in T} B_j \quad \text{для каждого} \quad T \in \mathbf{T}.$$

Доказательство. Рассмотрим матрицу $\hat{\mathbf{p}}((b, \delta)) = (\hat{p}_{\theta, \theta'}((b, \delta)))$. Очевидно, что

$$\hat{p}_{\theta, \theta'}((b, \delta)) = \hat{p}_{\theta, \theta'}(b) = \begin{cases} 1, & \text{если } \theta' = \theta^b, \\ 0, & \text{если } \theta' \neq \theta^b. \end{cases} \quad (8)$$

Для всех $\theta \in V_n^\times$, $W \subseteq V_n$ из равенства (8) вытекает, что

$$\widehat{p}_{\theta, W}((b, \delta)) = \sum_{\theta' \in W} \widehat{p}_{\theta, \theta'}(b) = \begin{cases} 1, & \text{если } \theta^b \in W, \\ 0, & \text{если } \theta^b \notin W. \end{cases} \quad (9)$$

Зафиксируем произвольное $j \in \{1, \dots, d\}$. Пусть $p_j = |B_j|$. Очевидно, что B_j — орбита некоторого элемента $\beta_j \in V_n^\times$ циклической группы $\langle b \rangle$, порожденной преобразованием b . Компонента связности $\bar{\Gamma}_j(b)$ — цикл длины p_j , причем $\text{Aut}(\bar{\Gamma}_j(b)) \leq GL_n$, $\text{Aut}(\bar{\Gamma}_j(b)) \cong \mathbb{Z}_{p_i}^+$. Из равенства (9) следует, что для любого элемента $\theta \in V_n^\times$ и каждой орбиты W циклической группы $\langle g_j \rangle$

$$\widehat{p}_{\theta, W}(b) = \begin{cases} 1, & \text{если } \theta \in W, \\ 0, & \text{если } \theta \notin W. \end{cases} \quad (10)$$

Из определения 4 и равенства (10) вытекает $\oplus_{\mathbf{W}}$ -марковость преобразования b для разбиения

$$\mathbf{W} = \{\{\vec{0}_n\}\} \cup \bigcup_{i=1}^d \{W_i^{(1)}, \dots, W_i^{(t_i)}\}.$$

Кроме того, из равенства (9) вытекает справедливость равенства (10) для каждого множества W , являющегося объединением любых орбит циклической группы $\langle b \rangle$ на $V_n^\times$. Значит, (b, δ) является $\oplus_{\mathbf{W}_T}$ -марковским преобразованием для разбиения

$$\mathbf{W}_T = \{\{\vec{0}_n\}\} \cup \bigcup_{T \in \mathbf{T}} \{\tilde{B}_T\},$$

где $\mathbf{T}$ — любое разбиение множества $\{1, \dots, d\}$. $\square$

Сформулируем критерий $\oplus_{\mathbf{W}}$ -марковости произвольного аффинного преобразования $h \in AGL_n$ и укажем возникающее при этом условие на разбиение $\mathbf{W}$ пространства V_n , $\mathbf{W} \neq \{\{\vec{0}_n\}, V_n^\times\}$.

Следствие 2. Пусть $n \geq 2$, (b, δ) — произвольное аффинное преобразование на V_n , заданное условием

$$(b, \delta): \alpha \mapsto \alpha^b \oplus \delta, \quad b \in GL_n, \quad \delta \in V_n.$$

Преобразование (b, δ) является $\oplus_{\mathbf{W}}$ -марковским для нетривиального разбиения $\mathbf{W}$ пространства V_n ($\mathbf{W} \neq \{\{\vec{0}_n\}, V_n^\times\}$) тогда и только тогда, когда преобразование b сохраняет разбиение $\mathbf{W}$.

Доказательство. Согласно определению 4 преобразование (b, δ) является $\oplus_{\mathbf{W}}$ -марковским тогда и только тогда, когда $\widehat{p}_{\theta, W}((b, \delta)) = \widehat{p}_{\theta', W'}((b, \delta))$ для всех $W, W' \in \mathbf{W}$ и всех $\theta, \theta' \in W$.

Из равенства (9) следует, что данное условие выполняется тогда и только тогда, когда либо $W' = W^b$, либо $W' \cap W^b = \emptyset$. Отсюда вытекает, что преобразование (b, δ) является $\oplus_{\mathbf{W}}$ -марковским тогда и только тогда, когда $\mathbf{W}^b = \mathbf{W}$. $\square$

Сформулируем критерий абсолютной немарковости аффинных преобразований из AGL_n .

Следствие 3. Пусть $n \geq 2$, (b, δ) — произвольное аффинное преобразование на V_n , заданное условием

$$(b, \delta): \alpha \mapsto \alpha^b \oplus \delta, \quad b \in GL_n, \quad \delta \in V_n.$$

Преобразование (b, δ) является абсолютно немарковским тогда и только тогда, когда $2^n - 1$ — простое число и граф $\bar{\Gamma}(b) = (V_n^\times, \{(\alpha, \alpha^b) \mid \alpha \in V_n^\times\})$ сильно связан.

Доказательство. Из утверждения 4 вытекает, что если $2^n - 1$ — не простое число или граф $\bar{\Gamma}(b)$ не связан, то существует такое нетривиальное разбиение $\mathbf{W}$ пространства V_n , $\mathbf{W} \neq \{\{\vec{0}_n\}, V_n^\times\}$, что (b, δ) — $\oplus_{\mathbf{W}}$ -марковское преобразование.

Пусть теперь граф $\bar{\Gamma}(b) = (V_n^\times, \{(\alpha, \alpha^b) \mid \alpha \in V_n^\times\})$ сильно связан, $2^n - 1$ — простое число и существует такое нетривиальное разбиение $\mathbf{W}$ пространства V_n , что (b, δ) — $\oplus_{\mathbf{W}}$ -марковское преобразование и

$$\mathbf{W} \neq \{\{\vec{0}_n\}, V_n^\times\}.$$

Тогда согласно следствию 2 должно выполняться равенство $\mathbf{W}^b = \mathbf{W}$.

Значит, для каждого блока $W \in \mathbf{W}$, $\vec{0}_n \notin W$, справедливо включение

$$W^{(b)} \subset \mathbf{W}. \quad (11)$$

Однако из простоты числа $2^n - 1$ и сильной связности графа $\bar{\Gamma}(b)$ вытекает невозможность выполнения включения (11) для каждого блока $W \in \mathbf{W}$. $\square$

Известно (см., например, [20]), что характеристический многочлен линейного преобразования b имеет максимальный период, если граф $\bar{\Gamma}(b)$ линейного преобразования b сильно связан. Поэтому критерий абсолютной немарковости, приведенный в следствии 3, можно сформулировать следующим образом. Преобразование (b, δ) является абсолютно немарковским тогда и только тогда, когда число $2^n - 1$ простое, а характеристический многочлен линейного преобразования b имеет максимальный период.

Из следствия 3 вытекает, что если преобразование $b \in GL_n$ имеет цикл длины $2^n - 1$, причем число $2^n - 1$ простое, то аффинное преобразование

$$(b, \delta): \alpha \mapsto \alpha^b \oplus \delta, \quad b \in GL_n, \quad \delta \in V_n,$$

абсолютно немарковское. Поэтому для каждого $n \in \{3, 5, 7, 31\}$ существуют абсолютно немарковские аффинные преобразования из AGL_n . Однако для любого натурального $m \geq 2$ (при $n = 2^m$) каждое аффинное преобразование из AGL_{2^m} является относительно марковским.

Пример 7. Подстановка $s \in S(V_3)$ является абсолютной немарковской тогда и только тогда, когда $s = (b, \delta)$ — такое преобразование из AGL_3 , что граф $\bar{\Gamma}(b)$ сильно связан.

Доказательство получено полным перебором всех подстановок из $S(V_3)$ и всех возможных разбиений множества $V_3^\times$.

5. $\oplus_W$ -марковость преобразований, наделенных дополнительными свойствами

Для $m, d \in \mathbb{N}$, $n = md$ и $\alpha = (\alpha_{d-1}, \dots, \alpha_0) \in \mathbb{Z}_{2^m}^d$, $\beta = (\beta_{d-1}, \dots, \beta_0) \in \mathbb{Z}_{2^m}^d$ положим

$$\alpha +_{2^m} \beta = ((\alpha_{d-1} + \beta_{d-1})_{2^m}, \dots, (\alpha_0 + \beta_0)_{2^m}).$$

Таким образом, $+_{2^m}$ — операция покомпонентного сложения в $\mathbb{Z}_{2^m}$ -модуле $\mathbb{Z}_{2^m}^d$; это обозначение используется также и для сложения в кольце $\mathbb{Z}_{2^m}$ (по аналогии с операцией $\oplus$). В алгоритме блочного шифрования $+_{2^m}$ — операция сложения текста с ключом, а аддитивная группа $\mathbb{Z}_{2^m}$ -модуля $\mathbb{Z}_{2^m}^d$ — группа наложения ключа. Так, если $m = 1$, то $d = n$, $\oplus = +_2$ и $V_n = \mathbb{Z}_2^n$.

Опишем классы $+_W$ -марковских аффинных преобразований для разбиений W $\mathbb{Z}_{2^m}$ -модуля $\mathbb{Z}_{2^m}^d$. Такие преобразования могут являться компонентами раундовой функции $+_{2^m}$ -марковского алгоритма блочного шифрования, например использоваться в линейном слое, а также быть составной частью преобразования нелинейного слоя.

Утверждение 5. Пусть $n = md$, $m, d \in \mathbb{N}$. Аффинное преобразование $h = (h_0, \lambda) \in GL_d(\mathbb{Z}_{2^m}) \times \mathbb{Z}_{2^m}^d$, заданное условием $h: \alpha \mapsto \alpha^{h_0} +_{2^m} \lambda$, является $+_{2^m} W$ -марковским для разбиения W $\mathbb{Z}_{2^m}$ -модуля $\mathbb{Z}_{2^m}^d$ тогда и только тогда, когда h_0 сохраняет W .

Доказательство следует из справедливости равенств

$$\hat{p}_{\theta, \theta^{h_0}}(h) = 1, \quad \hat{p}_{\theta, W}(h) = \mathbf{I}\{\theta^{h_0} \in W\} \quad (12)$$

для всех $\theta \in \mathbb{Z}_{2^m}^d$, $W \subseteq \mathbb{Z}_{2^m}^d$. $\square$

Рассмотрим заданное условием (12) произвольное аффинное преобразование $h = (h_0, \lambda) \in GL_d(\mathbb{Z}_{2^m}) \times \mathbb{Z}_{2^m}^d$. Пусть t — число орбит преобразования h_0 на $\mathbb{Z}_{2^m}^d$, U_j — j -я орбита h_0 , $j = 0, \dots, t-1$. Приведем примеры разбиений $\mathbf{W}$, относительно которых преобразование h является $+_{2^m}\mathbf{W}$ -марковским. Из утверждения 5 следует, что такие разбиения $\mathbf{W}$ суть:

1. $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$, где $W_j = \bigcup_{i \in J_j} U_i$, $J = \{J_0, \dots, J_{r-1}\}$ — произвольное разбиение (в том числе тривиальное) множества $\{0, \dots, t-1\}$, $r \leq t$.
2. $\bigcup_{i=0}^{t-1} \bigcup_{U \in \mathbf{U}^{(i)}} \{U\}$, где $\mathbf{U}^{(j)}$ — произвольное разбиение j -й орбиты U_j , сохраняемое h_0 , $j = 0, \dots, t-1$.

Пусть теперь $d = n$, $m = 1$ и $h = (h_0, \lambda) \in AGL_n$ задано условием (12). Если h_0 приводимо, то п. 1 включает разбиение $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$, блоками которого являются смежные классы по инвариантному подпространству W_0 преобразования h_0 . Из утверждения 5 следует, что преобразование h может являться $\oplus_{\mathbf{W}}$ -марковским также и для разбиений $\mathbf{W}$ пространства V_n , блоки которых не являются смежными классами по некоторой подгруппе группы V_n^+ , т.е. блоками некоторой системы импримитивности. В частности, существуют $\oplus_{\mathbf{W}}$ -марковские преобразования h с примитивной группой $C_n(h) = \langle h, V_n^+ \rangle$. Из утверждения 5 также следует, что для каждого разбиения $\mathbf{W}$ пространства V_n множество всех $\oplus_{\mathbf{W}}$ -марковских преобразований из AGL_n является группой, которую обозначим через $AGL_n^{(\mathbf{W})}$.

В общем случае из $\oplus_{\mathbf{W}}$ -марковости преобразований $b_1, b_2 \in S(V_n)$ для некоторого разбиения $\mathbf{W}$ пространства V_n не следует $\oplus_{\mathbf{W}}$ -марковость преобразования $b_1 b_2$. Для произвольного разбиения $\mathbf{W}$ и $\oplus_{\mathbf{W}}$ -марковских преобразований $b_1, b_2 \in S(V_n)$ приведем пример $\oplus_{\mathbf{W}}$ -марковской раундовой функций, компонентами которой являются b_1, b_2 . Сформулируем условия, при которых раундовая функция XSL-алгоритма является $\oplus_{\mathbf{W}}$ -марковской.

Пусть $v \in S(V_n)$, а частичная функция $g_k^{(v)}: V_n \rightarrow V_n$ задана условием

$$g_k^{(v)}: \alpha \mapsto (\alpha \oplus k)^v \quad \text{для всех } (\alpha, k) \in V_n^2.$$

Утверждение 6. Пусть $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ — разбиение пространства V_n . Тогда:

1. Если s — $\oplus_{\mathbf{W}}$ -марковская подстановка на V_n , то для каждого элемента $b \in (AGL_n^{(\mathbf{W})})_s(AGL_n^{(\mathbf{W})})$ алгоритм блочного шифрования с раундовой функцией $g^{(b)}$ и преобразование b являются $\oplus_{\mathbf{W}}$ -марковскими.

2. Если $d \in \mathbb{N}$, $s_1, \dots, s_d$ — $\oplus_{\mathbf{W}}$ -марковские подстановки на V_n , а частичная раундовая функция $\tilde{g}_{(k^{(1)}, \dots, k^{(d)})}^{(d)}: V_n \rightarrow V_n$ задана условием

$$\tilde{g}_{(k^{(1)}, \dots, k^{(d)})}^{(d)} = g_{k^{(1)}}^{(s_1)} \cdots g_{k^{(d)}}^{(s_d)} \quad \text{для всех } (k^{(1)}, \dots, k^{(d)}) \in V_n^d,$$

то алгоритм блочного шифрования с раундовой функцией $\tilde{g}^{(d)}$ является $\oplus_{\mathbf{W}}$ -марковским.

Доказательство. Заметим, что для любой подстановки $v \in S(V_n)$ справедливо равенство

$$p_{\varepsilon, W}(g^{(v)}) = \widehat{p}_{\varepsilon, W}(v) \quad \text{для всех } (\varepsilon, W) \in V_n \times \mathbf{W}. \quad (13)$$

1. Из утверждения 2 вытекает $\oplus_{\mathbf{W}}$ -марковость преобразования b . Из равенства (13), $\oplus_{\mathbf{W}}$ -марковости преобразования b следует $\oplus_{\mathbf{W}}$ -марковость алгоритма блочного шифрования с раундовой функцией $g^{(b)}$.

2. Из равенства (13), $\oplus_{\mathbf{W}}$ -марковости подстановок $s_1, \dots, s_d$ и утверждения 3 [2] следует $\oplus_{\mathbf{W}}$ -марковость алгоритма блочного шифрования с раундовой функцией $\tilde{g}^{(d)}$. $\square$

Для разбиения $\mathbf{W}$ множества X одного вида опишем класс $\otimes_{\mathbf{W}}$ -марковских преобразований, являющихся также $\otimes_{\mathbf{W}'}$ -марковскими для каждого укрупнения $\mathbf{W}'$.

Пусть μ — $(d+1)$ -значная метрика на V_n , принимающая все значения из множества $\{0, \dots, d\}$ и инвариантная относительно V_n^+ . Отметим, что такая $(d+1)$ -значная метрика μ однозначно определяется разбиением $\{A_1, \dots, A_d\}$ множества $V_n^\times$, где $A_j = \{\alpha \in V_n \mid \mu(\vec{0}_n, \alpha) = j\}$ для всех $j \in \{1, \dots, d\}$, и задается условиями

$$\mu(\alpha, \alpha') = i, \quad \text{если } \alpha \oplus \alpha' \in A_i, \quad i = 1, 2, \dots, d. \quad (14)$$

Опишем такие разбиения $\mathbf{W} = \{\{\vec{0}_n\}, W_1, \dots, W_{d-1}\}$ пространства V_n , что существуют $\oplus_{\mathbf{W}}$ -марковские преобразования, принадлежащие группе изометрий $\text{Isom}(\mu)$. Они являются еще одним примером $\oplus_{\mathbf{W}}$ -марковских преобразований, у которых:

- 1) блоки разбиения $\mathbf{W}$ не равномощны, в частности они не являются смежными классами по некоторой подгруппе $H < (V_n, \oplus)$,
- 2) на группу $\text{Isom}(\mu)$, кроме условия $V_n^+ \leq \text{Isom}(\mu)$, не накладываются никакие дополнительные ограничения, вытекающие из $\oplus_{\mathbf{W}}$ -марковости преобразований, в частности она может быть примитивной.

Далее будет показано, что из условий $V_n^+ \leq \text{Isom}(\mu)$ и $b \in \text{Isom}(\mu)$ вытекает $\oplus_{\mathbf{W}}$ -марковость преобразования b для разбиения $\mathbf{W}$, определяющего нетривиальную метрику μ посредством равенства (14). Данное свойство позволяет указать большой класс преобразований, которые являются $\oplus_{\mathbf{W}'}$ -марковскими для фиксированного разбиения $\mathbf{W}'$.

Далее для формулировки утверждения понадобится понятие подметрики метрики (см. [21]).

Определение 9 ([21]). Пусть μ — конечная метрика на множестве X . Метрика $\rho_\mu: X^2 \rightarrow \mathbb{N}_0$, удовлетворяющая для всех $\alpha, \beta, \gamma, \delta \in X$ условиям

- 1) если $\mu(\alpha, \beta) = \mu(\gamma, \delta)$, то $\rho_\mu(\alpha, \beta) = \rho_\mu(\gamma, \delta)$,
- 2) $\rho_\mu(\alpha, \beta) \leq \mu(\alpha, \beta)$,

называется подметрикой метрики μ .

Метрика Хемминга и ее подметрики (см. [21]) являются примерами метрик, задаваемых условием (14).

Следующий результат полезен при описании наследования свойства $\oplus_{\mathbf{W}}$ -марковости подстановки b при объединении блоков разбиения $\mathbf{W}$. В частности, он будет использован (утверждение 7) для указания связи между существованием подметрик вида (14) и возможностью дальнейшего укрупнения $\mathbf{W}'$ блоков разбиения $\mathbf{W}$, относительно которого подстановка b является также $\otimes_{\mathbf{W}'}$ -марковской.

Лемма. Пусть:

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

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

Подстановка b является $\otimes_{\mathbf{W}'}$ -марковской тогда и только тогда, когда

$$J_i^s = J_c \quad \text{или} \quad J_i^s \cap J_c = \emptyset \quad \text{для любых } i, c \in \{0, \dots, d-1\}. \quad (15)$$

В этом случае $\hat{\mathbf{p}}_{\mathbf{W}'}(b)$ — также подстановочная матрица.

Доказательство. Так как $\widehat{\mathbf{p}}_{\mathbf{W}}(b)$ — подстановочная матрица, то для некоторой подстановки $s \in S(\{0, \dots, r-1\})$ справедливо равенство $\widehat{\mathbf{p}}_{\mathbf{W}}(b) = \mathbf{q}(s) = (q_{i,j}(s))$, где

$$q_{i,j}(s) = \begin{cases} 1, & \text{если } j = i^s, \\ 0, & \text{если } j \neq i^s. \end{cases} \quad (16)$$

Зафиксируем произвольные $i \in \{0, \dots, r-1\}$, $\theta \in W_i$. Из равенства (16) следует, что для произвольного $t \in \{0, \dots, r-1\}$

$$\widehat{p}_{\theta, W_t}(b) = \begin{cases} 1, & \text{если } t = i^s, \\ 0, & \text{если } t \neq i^s. \end{cases} \quad (17)$$

Следовательно, для каждого $c \in \{0, \dots, d-1\}$ справедливо равенство

$$\widehat{p}_{\theta, W'_c}(b) = \sum_{j \in J_c} \widehat{p}_{\theta, W_j}(b) = \mathbf{I}\{i^s \in J_c\}. \quad (18)$$

Покажем, что из условия (15) вытекает $\otimes_{\mathbf{W}'}$ -марковость подстановки b . Зафиксируем произвольный блок $J_t \in \mathbf{J}$ и произвольные $i_1, i_2 \in J_t$. Из условия (15) вытекает справедливость равенства $J_t^s = J_c$ для некоторого $c \in \{0, \dots, d-1\}$, а также $J_t^s \cap J_i = \emptyset$ для каждого $i \in \{0, \dots, d-1\} \setminus \{c\}$. Значит,

$$\mathbf{I}\{i_1^s \in J_i\} = \mathbf{I}\{i_2^s \in J_i\} \quad \text{для каждого } i \in \{0, \dots, d-1\}.$$

Тогда из равенства (18) имеем

$$\widehat{p}_{\theta, W'}(b) = \widehat{p}_{\theta', W'}(b) \quad \text{для любых } (\theta, \theta') \in W_{i_1} \times W_{i_2}, \quad W' \in \mathbf{W}',$$

причем $W_{i_1}, W_{i_2} \subseteq W'_t$. Поэтому из определения 4 следует $\otimes_{\mathbf{W}'}$ -марковость подстановки b .

Покажем, что из $\otimes_{\mathbf{W}'}$ -марковости подстановки b вытекает условие (15). Так как $\mathbf{W}'$ — нетривиальное укрупнение разбиения $\mathbf{W}$, то существует такое $i \in \{0, \dots, d-1\}$, что $|J_i| \geq 2$. Если подстановка b является $\otimes_{\mathbf{W}'}$ -марковской, то для каждой пары $(i_1, i_2) \in J_i^2$, а также для произвольных $(\theta_1, \theta_2) \in W_{i_1} \times W_{i_2}$, $c = 0, \dots, d-1$, справедливо равенство $\widehat{p}_{\theta_1, W'_c}(b) = \widehat{p}_{\theta_2, W'_c}(b)$, которое согласно равенству (18) равносильно условию

$$\mathbf{I}\{i_1^s \in J_c\} = \mathbf{I}\{i_2^s \in J_c\}.$$

Отсюда вытекают условия

$$J_i^s \subseteq J_c \quad \text{или} \quad J_i^s \cap J_c = \emptyset \quad \text{для любых } i, c \in \{0, \dots, d-1\}.$$

Следовательно, подмножество J_c для каждого $c \in \{0, \dots, d-1\}$ является блоком циклической группы $\langle s \rangle$. Поэтому справедливо условие (15). $\square$

Утверждение 7. Пусть разбиение $\{A_1, \dots, A_d\}$ множества $V_n^\times$ таково, что $(d+1)$ -значная метрика μ на V_n задана условием (14). Тогда каждое преобразование $b \in \text{Isom}(\mu)$ является $\oplus_{\mathbf{W}}$ -марковским для разбиения $\mathbf{W} = \{\{\vec{0}_n\}, A_1, \dots, A_d\}$ с единичной матрицей $\hat{\mathbf{p}}_{\mathbf{W}}(b)$. Кроме того, преобразование $b \in \text{Isom}(\mu)$ является $\oplus_{\mathbf{W}'}$ -марковским для каждого такого укрупнения $\mathbf{W}'$ разбиения $\mathbf{W}$, что разбиение $\mathbf{W}' = \{\{\vec{0}_n\}, A'_1, \dots, A'_r\}$ задает подметрику μ' метрики μ условиями

$$\mu'(\alpha, \alpha') = i, \quad \text{если} \quad \alpha \oplus \alpha' \in A'_i, \quad i = 1, 2, \dots, r, \quad r < d.$$

Доказательство. Из задания метрики μ условием (14) и включения $b \in \text{Isom}(\mu)$ вытекает равенство

$$\alpha^b \oplus (\alpha \oplus A_i)^b = A_i \quad \text{для каждого} \quad \alpha \in V_n, \quad i = 1, 2, \dots, d.$$

Поэтому для всех $\theta \in V_n^\times$, $i \in \{1, \dots, d\}$ справедливо равенство

$$\hat{p}_{\theta, A_i}(b) = \begin{cases} 1, & \text{если} \quad \theta \in A_i, \\ 0, & \text{если} \quad \theta \notin A_i. \end{cases} \quad (19)$$

Из равенства (19) вытекает $\oplus_{\mathbf{W}}$ -марковость преобразования b относительно разбиения $\mathbf{W} = \{\{\vec{0}_n\}, A_1, \dots, A_d\}$, при этом матрица $\hat{\mathbf{p}}_{\mathbf{W}}(b)$ является единичной.

Из леммы 1 вытекает $\oplus_{\mathbf{W}'}$ -марковость преобразования b для укрупнения $\mathbf{W}'$, соответствующего подметрике μ' . $\square$

Авторы благодарны И. А. Круглову за полезные замечания.

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] Погорелов Б. А., Пудовкина М. А., “О расстояниях от подстановок до импримитивных групп при фиксированной системе импримитивности”, *Дискретная математика*, **25:3** (2013), 78–95.

- [5] Погорелов Б. А., Пудовкина М. А., “О расстояниях от подстановок до объединения всех импримитивных групп с равными параметрами систем импримитивности”, *Дискретная математика*, **26**:1 (2014), 103–117.
- [6] Кемени Д., Снелл Д., *Конечные цепи Маркова*, М.: Наука, 1970, 272 с.
- [7] Черемушкин А. В., “Методы аффинной и линейной классификации двоичных функций”, *Труды по дискретной математике*, **4** (2001), 273–314.
- [8] Biryukov A., Canniere C., Braeken A., Preneel B., “A toolbox for cryptanalysis: linear and affine equivalence algorithms”, EUROCRYPT 2003, Lect. Notes Comput. Sci., **2656**, 2003, 33–50.
- [9] Leander G., Poschmann A., “On the classification of 4-bit S -boxes”, WAIFI 2007, Lect. Notes Comput. Sci., **4547**, 2007, 159–176.
- [10] Saarinen M.-J. O., “Cryptographic analysis of all 4×4 -bit S -boxes”, SAC 2011, Lect. Notes Comput. Sci., **7118**, 2012, 118–133.
- [11] Sarkar S., Maitra S., Chakraborty K., “Differential power analysis in Hamming weight model: how to choose among (extended) affine equivalent S -boxes”, INDOCRYPT 2014, Lect. Notes Comput. Sci., **8885**, 2014, 360–373.
- [12] Cheng L., Zhang W., Xiang Z., “A new cryptographic analysis of 4-bit S -boxes”, INSCRYPT 2015, Lect. Notes Comput. Sci., **9589**, 2016, 144–164.
- [13] Nyberg K., Knudsen L. R., “Provable security against differential cryptanalysis”, CRYPTO 1992, Lect. Notes Comput. Sci., **740**, 1993, 566–574.
- [14] Budaghyan L., *Construction and Analysis of Cryptographic Functions*, Heidelberg etc.: Springer, 2014, viii+172 с.
- [15] Canteaut A., Duval S., Leurent G., “Construction of lightweight S -boxes using Feistel and Misty structures”, SAC 2015, Lect. Notes Comput. Sci., **9566**, 2016, 373–393.
- [16] Canteaut A., Roue J., “On the behaviors of affine equivalent S -boxes regarding differential and linear attacks”, EUROCRYPT 2015, Part I, Lect. Notes Comput. Sci., **9056**, 2015, 45–74.
- [17] Ivanov G., Nikolov N., Nikova S., “Reversed genetic algorithms for generation of bijective S -boxes with good cryptographic properties”, *Cryptography and Communication*, **8** (2016), 247–276.
- [18] Глухов М. М., “О матрицах переходных разностей при использовании некоторых модульных групп”, *Математические вопросы криптографии*, **4**:4 (2013), 27–47.
- [19] *Дискретная математика. Энциклопедия*, М.: Научное издательство «Большая Российская энциклопедия», 2004, 382 с.
- [20] Глухов М. М., Елизаров В. П., Нечаев А. А., *Алгебра: Учебник. В 2-х т. Т. II*, М.: Гелиос АРВ, 2003, 416 с.
- [21] Погорелов Б. А., “Подметрики метрики Хемминга и теорема А. А. Маркова”, *Труды по дискретной математике*, **9** (2006), 190–219.