Б. А. Погорелов, М. А. Пудовкина, Разбиения на биграммах и марковость алгоритмов блочного шифрования, *Матем. вопр. криптогр.*, 2017, том 8, выпуск 1, 107–142

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2017 Т. 8 № 1 С. 107–142

УДК 519.719.2+519.712

Разбиения на биграммах и марковость алгоритмов блочного шифрования

Б. А. Погорелов [1], **М. А. Пудовкина** [2]

[1] *Академия криптографии Российской Федерации, Москва*

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

Получено 20.IV.2015

Аннотация. Изучается модель итерационных алгоритмов блочного шифрования с независимыми и равновероятно выбираемыми раундовыми ключами, алфавитом текстов X и группой $(X, \otimes)$ наложения ключа. Указаны условия, обеспечивающие сохранение марковости при укрупнении цепи Маркова с множеством состояний X^2, соответствующей биграммам промежуточных текстов. Описаны свойства рассматриваемых марковских алгоритмов блочного шифрования и преобразований укрупнения.

Ключевые слова: марковский алгоритм блочного шифрования, цепи Маркова, укрупнение состояний, метод усеченных разностей

Partitions on bigrams and Markov property of block ciphers

B. A. Pogorelov [1], **M. A. Pudovkina** [2]

[1] *Academy of Cryptograpfy of the Russian Federation, Moscow*

[2] *Bauman Moscow State Technical University, Moscow*

Abstract. A model of iterated block ciphers with alphabet X, independent uniform round keys and a key addition group $(X, \otimes)$ is considered. We find conditions ensuring the preservation of Markov property under lumping of Markov chain with state space X^2 corresponding to bigrams of intermediate ciphertexts. We describe properties of Markov ciphers considered and lumping transforms.

Key words: Markov block cipher, Markov chain, states lumping, truncated differential technique

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 1, pp. 107–142 (Russian)

1. Введение

Некоторые вероятностные методы криптоанализа алгоритмов блочного шифрования [1], в том числе разностный метод и его обобщения, основаны на построении l-раундовой характеристики, слабо зависящей от ключа. Как правило, они применимы к блочным шифрсистемам, имеющим итерационную функцию зашифрования, которая является композицией раундовых функций.

Число таких частичных раундовых функций называется *числом раундов*, а саму функцию зашифрования, состоящую из l раундов, называют *l-раундовой*. Для l-раундовой функции зашифрования с алфавитом текстов X фиксируется некоторое натуральное число $t \in \mathbb{N}$ и рассматриваются декартово произведение X^t и последовательность его разбиений $\mathbf{X}^{(0)}, \ldots, \mathbf{X}^{(l)}$, где разбиение $\mathbf{X}^{(i)} = \{X_0^{(i)}, \ldots, X_{r^{(i)}-1}^{(i)}\}$ состоит из $r^{(i)}$ блоков (подмножеств)

$$X_0^{(i)}, \ldots, X_{r^{(i)}-1}^{(i)}, \quad r^{(i)} \geqslant 1, \quad i = 0, \ldots, l.$$

Элементы множества X^t будем называть *t-граммами* текстов. Для каждого раунда i ищется вероятность $p_{X_{c_{i-1}}^{(i-1)}, X_{c_i}^{(i)}}(g^{(i)})$ перехода элементов блока $X_{c_{i-1}}^{(i-1)} \in \mathbf{X}^{(i-1)}$ в элементы блока $X_{c_i}^{(i)} \in \mathbf{X}^{(i)}$ под действием раундовой функции $g^{(i)} \colon X \times K^{(i)} \to X$ в предположении, что раундовый ключ $k^{(i)}$ выбирается случайно и равновероятно из множества $K^{(i)}$ всех раундовых ключей i-го раунда, где $c_i \in \{0, \ldots, r^{(i)} - 1\}$, $i \in \{0, \ldots, l\}$.

При фиксированных номерах $c_0, \ldots, c_l$ последовательность блоков $X_{c_0}^{(0)}, \ldots, X_{c_l}^{(l)}$ будем называть *l-раундовой характеристикой*. Она соответствует реализации последовательности случайных величин. Так, в разностном методе $t = 2$, $(X, \otimes)$ — группа с операцией сложения $\otimes$,

$$\mathbf{X} = \mathbf{X}^{(0)} = \ldots = \mathbf{X}^{(l)} = \{X_\varepsilon \,|\, \varepsilon \in X\},$$

где

$$X_\varepsilon = \big\{(\varepsilon \otimes \alpha, \alpha) \,\big|\, \alpha \in X\big\} \quad \text{для} \quad \varepsilon \in X, \quad i = 0, \ldots, l.$$

Последовательность блоков $X_{\theta^{(0)}}, \ldots, X_{\theta^{(l)}}$ отождествляется с последовательностью их номеров $\theta^{(0)}, \ldots, \theta^{(l)} \in X$, называемых разностями. Блоки разбиения $\mathbf{X}$ множества X^2 суть множества минимальной мощности, инвариантные относительно операции $\otimes$ наложения раундового ключа. Все остальные разбиения множества X^2, инвариантные относительно такого наложения раундового ключа, получаются объединением блоков разбиения $\mathbf{X}$.

Далее при криптоанализе используется марковская модель, основанная на предположении о независимости раундовых ключей. Тогда вероятность перехода для l-раундовой характеристики $c_0 \xrightarrow{l} c_l$ (перехода элементов c_0-го блока $X_{c_0}^{(0)}$ t-грамм открытого текста в элементы c_l-го блока $X_{c_l}^{(l)}$ t-грамм шифртекста под действием l-раундовой функции зашифрования) равна

$$p_{X_{c_0},X_{c_l}}^{(l)} = \sum_{t_1=0}^{r^{(1)}-1} \sum_{t_2=0}^{r^{(2)}-1} \cdots \sum_{t_{l-1}=0}^{r^{(l-1)}-1} \prod_{i=1}^{l} p_{X_{t_{i-1}}^{(i-1)},X_{t_i}^{(i)}}(g^{(i)}), \quad t_0 = c_0, \ t_l = c_l.$$

Однако на практике из-за большого объема вычислений вероятность $p_{X_{c_0},X_{c_l}}^{(l)}$ обычно оценивается снизу величиной

$$\widetilde{p}_{X_{c_0},X_{c_l}}^{(l)} = \prod_{i=1}^{l} p_{X_{c_{i-1}}^{(i-1)},X_{c_i}^{(i)}}(g^{(i)})$$

для одной фиксированной последовательности блоков $X_{c_0}^{(0)}, X_{c_1}^{(1)}, \ldots, X_{c_l}^{(l)}$, которую стараются подобрать таким образом, чтобы величина $\widetilde{p}_{X_{c_0},X_{c_l}}^{(l)}$ была наибольшей. Раундовой функции $g^{(i)}$ ставится в соответствие матрица

$$\mathbf{p}(g^{(i)}) = (p_{X^{(i-1)},X^{(i)}}(g^{(i)}))$$

вероятностей переходов элементов блоков разбиения $\mathbf{X}^{(i-1)}$ в элементы блоков разбиения $\mathbf{X}^{(i)}$ под действием $g^{(i)}$, $i = 1, \ldots, l$ (далее — матрица вероятностей переходов блоков). Матрица вероятностей переходов блоков разбиения t-грамм открытого текста $\mathbf{X}^{(0)}$ в блоки разбиения $\mathbf{X}^{(l)}$ t-грамм шифртекста под действием функции зашифрования предполагается равной $\prod_{i=1}^{l} \mathbf{p}(g^{(i)})$.

Для справедливости данного предположения достаточно, чтобы рассматриваемая случайная последовательность, соответствующая промежуточным t-граммам блоков разбиений, являлась цепью Маркова. Далее будем называть *марковской* последовательность случайных величин, являющуюся цепью Маркова. Так, в разностном методе раундовой функции $g^{(i)}$ и разбиению $\mathbf{X}$ ставится в соответствие матрица вероятностей переходов разностей $\mathbf{p}(g^{(i)}) = (p_{\varepsilon,\delta}(g^{(i)}))$, где $p_{\varepsilon,\delta}(g^{(i)})$ — стандартное обозначение вероятности $p_{X_\varepsilon,X_\delta}(g^{(i)})$ перехода блока X_ε в блок X_δ под действием раундовой функции $g^{(i)}$ в предположении, что раундовый ключ выбирается случайно и равновероятно из множества $K^{(i)}$, $\varepsilon, \delta \in X$, $i = 1, \ldots, l$.

Для абелевой группы $(X, \otimes)$ в [2] рассматриваются итерационные алгоритмы блочного шифрования, названные $\otimes$-*марковскими*, у которых имеет место равенство

$$p_{\theta^{(i-1)},\theta^{(i)}}(g^{(i)}|\alpha) = p_{\theta^{(i-1)},\theta^{(i)}}(g^{(i)}) \quad \text{для всех пар} \quad (\theta^{(i-1)} \otimes \alpha, \alpha) \in X_{\theta^{(i-1)}}$$

при случайном и равновероятном выборе раундового ключа из множества $K^{(i)}$. В [2] доказано, что для таких алгоритмов последовательность разностей $\theta^{(0)}, \ldots, \theta^{(l)}$ является цепью Маркова.

В настоящей работе в рамках описанной модели алгоритмов блочного шифрования предлагается первоначально рассматривать последовательность случайных величин $\xi^{(0)}, \xi^{(1)}, \ldots, \xi^{(l)}$, соответствующую биграммам промежуточных текстов. Биграммы текстов можно считать состояниями конечного детерминированного автомата, на вход которого поступают раундовые ключи, а функции переходов задаются раундовыми функциями. В рамках автоматной модели (вероятностного преобразователя) элементарно получаем цепь Маркова с множеством состояний X^2 и матрицей вероятностей переходов, элементы которой заданы условием

$$p_{(\alpha_1,\alpha_0),(\alpha'_1,\alpha'_0)}(g^{(i)}) = \mathbf{P}\big\{\big(\alpha_1^{g_k^{(i)}}, \alpha_0^{g_k^{(i)}}\big) = (\alpha'_1, \alpha'_0)\big\},$$

где

$$g_k^{(i)} : \alpha \mapsto g^{(i)}(\alpha, k),$$

а раундовый ключ k выбирается случайно и равновероятно из множества $K^{(i)}$ и, естественно, независимо от биграмм (α_1, α_0), $(\alpha'_1, \alpha'_0) \in X^2$.

Описываются свойства различных укрупнений состояний марковской последовательности $\xi^{(0)}, \xi^{(1)}, \ldots, \xi^{(l)}$ с применением соответствующей теории цепей Маркова [3]. В частности, показано, что результаты работы [2] о марковости последовательности $\xi^{(0)}_{\mathbf{X}}, \xi^{(1)}_{\mathbf{X}}, \ldots, \xi^{(l)}_{\mathbf{X}}$, полученной из последовательности $\xi^{(0)}, \xi^{(1)}, \ldots, \xi^{(l)}$ укрупнением ее состояний посредством разбиения $\mathbf{X} = \{X_\varepsilon \,|\, \varepsilon \in X\}$ следуют из теоремы 6.3.2 в [3]. Приведены условия, при которых последовательность $\xi^{(0)}_{\mathbf{W}}$, $\xi^{(1)}_{\mathbf{W}}, \ldots, \xi^{(l)}_{\mathbf{W}}$, полученная посредством дальнейшего укрупнения состояний марковской последовательности $\xi^{(0)}_{\mathbf{X}}, \xi^{(1)}_{\mathbf{X}}, \ldots, \xi^{(l)}_{\mathbf{X}}$ разбиением $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$ множества X, также является марковской. Наоборот, можно рассматривать и промежуточные укрупнения между биграммами и разностями. Например,

$$X_{\varepsilon,W_j} = \big\{(\varepsilon \otimes \alpha, \alpha) \,|\, \alpha \in W_j\big\},$$

где $\{W_0, \ldots, W_{r-1}\}$ — разбиение множества X на смежные классы по подгруппе $(W_0, \otimes)$ группы $(X, \otimes)$.

Итерационные алгоритмы блочного шифрования, у которых последовательность $\xi^{(0)}_{\mathbf{W}}, \xi^{(1)}_{\mathbf{W}}, \ldots, \xi^{(l)}_{\mathbf{W}}$ является марковской, названы $\otimes_{\mathbf{W}}$-*марковскими*. Отметим, что свойствам цепей Маркова вероятностных преобразователей и итерационных преобразований посвящены также работы [4 – 6], а укрупнениям цепей Маркова — [7].

Неявно допущение о $\otimes_{\mathbf{W}}$-марковости алгоритма блочного шифрования для некоторого класса блоков разбиений множества X и наборов номеров таких блоков используется в методе усеченных разностей — в одном из наиболее распространенных обобщений разностного метода (см. [8 – 13]). В этом случае неявно полагают, что для l-раундовых итерационных $\otimes$-марковских алгоритмов шифрования вероятность $\mathbf{P}\{(A_{j^{(l)}}, \ldots, A_{j^{(0)}})\}$ набора усеченных разностей $(A_{j^{(l)}}, \ldots, A_{j^{(0)}})$ находится как $\prod_{i=0}^{l-1} p_{A_{j^{(i)}}, A_{j^{(i+1)}}}(g^{(i+1)})$, где $A_{j^{(i)}}$ — блок некоторого разбиения множества X, $i = 0, \ldots, l$. В ряде работ (см., например, [10, 12]) при применении метода усеченных разностей проверка корректности равенства

$$\mathbf{P}\big\{\big(A_{j^{(l)}}, \ldots, A_{j^{(0)}}\big)\big\} = \prod_{i=0}^{l-1} p_{A_{j^{(i)}}, A_{j^{(i+1)}}}\big(g^{(i+1)}\big)$$

проводится посредством вычислительных экспериментов. Так, в [12] показано, что экспериментальная оценка вероятности $\mathbf{P}\{(A_{j^{(l)}}, \ldots, A_{j^{(0)}})\}$ может быть больше найденной по формуле $\prod_{i=0}^{l-1} p_{A_{j^{(i)}}, A_{j^{(i+1)}}}(g^{(i+1)})$.

В XSL-алгоритмах блочного шифрования и алгоритмах шифрования Фейстеля с XSL-функцией усложнения марковость последовательности случайных величин $\xi^{(0)}_{\mathbf{W}}, \ldots, \xi^{(l)}_{\mathbf{W}}$ может редуцироваться к свойствам S-боксов и преобразования линейного слоя. В связи с этим введем понятие $\otimes_{\mathbf{W}}$-марковского преобразования, следующее из определения $\otimes_{\mathbf{W}}$-марковости алгоритма блочного шифрования. В качестве примеров в данной работе рассмотрены преобразования, основанные 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. Примерами $+_{\mathbf{W}}$-марковских преобразований являются подстановки S-боксов алгоритма блочного шифрования SAFER [14] и логарифмические подстановки. Для APN-преобразований получена связь между элементами группы автоморфизмов графа, соответствующего APN-преобразованию b, и заданием блоков разбиения $\mathbf{W}$, для которого b является $+_{\mathbf{W}}$-марковским преобразованием.

Структура работы. В разделе 2 приведены основные обозначения и понятия. Раздел 3 содержит определение $\otimes_{\mathbf{W}}$-марковских алгоритмов блочного шифрования, а также условия на разбиение $\mathbf{W}$ и элементы матриц вероятностей переходов разностей $\mathbf{p}(g^{(1)}), \ldots, \mathbf{p}(g^{(l)})$, при которых последовательность случайных величин $\xi^{(0)}_{\mathbf{W}}, \xi^{(1)}_{\mathbf{W}}, \ldots, \xi^{(l)}_{\mathbf{W}}$ является марковской. В разделах 4, 5 даны примеры $+_{\mathbf{W}}$-марковских преобразований, основанных на операциях экспоненцирования и логарифмирования в кольце $\mathbb{Z}_{2^d}$ и поле $GF(p)$. В разделе 6 описана связь между $\oplus_{\mathbf{W}}$-марковостью и свойствами APN-подстановок.

2. Основные обозначения и понятия

Будут использованы следующие обозначения: X — произвольное конечное множество; $P(X)$ — множество всех преобразований X; $S(X)$ — симметрическая группа на X; $(X, \otimes)$ — произвольная группа на множестве X с бинарной операцией $\otimes$ и единичным элементом e; $X^{\times} = X \backslash e$; $\alpha^g = \alpha g = g(\alpha)$ — образ элемента $\alpha \in X$ при действии на него подстановкой $g \in S(X)$; α^{-1} — обратный к α элемент относительно операции $\otimes$, $\alpha \otimes \beta^{-1} = \alpha \overline{\otimes} \beta$ для любых $\alpha, \beta \in X$; $K^{(i)}$ — множество всех раундовых ключей i-го раунда, $k^{(i)} \in K^{(i)}$;

$$g^{(i)} : X \times K \to X$$

— раундовая функция i-го раунда и

$$g^{(i)}_{k^{(i)}} : \alpha \mapsto g^{(i)}(\alpha, k^{(i)})$$

— частичная раундовая функция i-го раунда, где $x \in X$, $k^{(i)} \in K^{(i)}$;

$$f_{\vec{k}_t} = g^{(1)}_{k^{(1)}} \cdots g^{(t)}_{k^{(t)}} \quad \text{для} \quad \vec{k}_t = (k^{(1)}, \ldots, k^{(t)}) \in K^{(1)} \times \cdots \times K^{(t)};$$

$K = K^{(1)} = \cdots = K^{(l)}$; запись $\delta_1, \ldots, \delta_d \in_U X$ означает, что элементы $\delta_1, \ldots, \delta_d$ выбираются из множества X по схеме выбора с возвращением независимо, случайно и равновероятно; V_m — векторное пространство размерности m над полем $GF(2)$; $\oplus$ — операция покоординатного сложения векторов над полем $GF(2)$, $I(B)$ — индикатор выполнения условия B; $\langle \delta_1, \ldots, \delta_c \rangle$ — группа, порожденная элементами $\delta_1, \ldots, \delta_c$; $GL_m = GL_m(2)$ — полная линейная группа над $GF(2)$; $Z_n = \{0, \ldots, n-1\}$; $\mathbf{P}\{A\}$ — вероятность события A; $\vec{1}_n$ — n-мерный единичный вектор; $\vec{0}_n$ — n-мерный нулевой вектор; $[a, b] = \{x \in \mathbb{R} \,|\, a \leqslant x \leqslant b\}$.

Каждому вектору $\alpha = (\alpha_{n-1}, \dots, \alpha_1, \alpha_0) \in V_n$ можно сопоставить элемент $\widetilde{\alpha} = 2^{n-1}\alpha_{n-1} + \cdots + 2\alpha_1 + \alpha_0$ кольца $\mathbb{Z}_{2^n}$. Тогда на V_n можно определить операции сложения и умножения по модулю 2^n, а над кольцом $\mathbb{Z}_{2^n}$ — операцию $\oplus$ векторного сложения векторов. Эти операции будем обозначать теми же знаками, что и соответствующие операции над числами или векторами. Из контекста всегда будет ясно, об операциях каких алгебраических структур идет речь.

Для случайных величин $\lambda_0, \dots, \lambda_d$ со значениями в множестве X обозначим $\lambda^{(d,\dots,0)} = (\lambda_d, \dots, \lambda_0)$ и $\lambda^{(d,\dots,0)} = \theta^{(d,\dots,0)}$, если $\lambda_d = \theta_d, \dots, \lambda_0 = \theta_0$, где $\theta^{(d,\dots,0)} = (\theta_d, \dots, \theta_0) \in X^{d+1}$.

Для произвольных элементов $\theta, \varepsilon \in X$ положим

$$p_{\theta,\varepsilon}(g) = \frac{1}{|K|\,|X|}\,\bigl|\{(\alpha, k) \in X \times K \bigm| (\theta \otimes \alpha)^{g_k} = \varepsilon \otimes \alpha^{g_k}\}\bigr|,$$

$$p_{\theta,\varepsilon}(g\,|\,\beta) = \frac{1}{|K|}\,\bigl|\{k \in K \bigm| (\theta \otimes \beta)^{g_k} = \varepsilon \otimes \beta^{g_k}\}\bigr|, \quad \beta \in X,$$

$$p^{(i)}_{\theta,\varepsilon} = \frac{1}{|X|}\prod_{j=1}^{i}\frac{1}{|K^{(j)}|}\,\Bigl|\Bigl\{(\alpha, \vec{k}_i) \in X \times \prod_{j=1}^{i} K^{(j)} \Bigm| (\theta \otimes \alpha)^{f_{\vec{k}_i}} = \varepsilon \otimes \alpha^{f_{\vec{k}_i}}\Bigr\}\Bigr|.$$

Если $p^{(i)}_{\theta,\varepsilon} > 0$, то пара (θ, ε) называется *i-раундовой разностью*, при $p^{(i)}_{\theta,\varepsilon} = 0$ пара (θ, ε) — *i-раундовая невозможная разность*.

Матрица $\mathbf{p}(g) = (p_{\theta,\varepsilon}(g))$ называется *матрицей вероятностей переходов разностей* раундовой функции g.

О п р е д е л е н и е 1. Алгоритм блочного шифрования с l-раундовой частичной функцией зашифрования

$$f_{\vec{k}_l} = g^{(1)}_{k^{(1)}} \cdots g^{(l)}_{k^{(l)}}$$

на ключе

$$\vec{k}_l = (k^{(1)}, \dots, k^{(l)}) \in K^{(1)} \times \cdots \times K^{(l)}$$

называется *l-раундовым итерационным алгоритмом блочного шифрования*.

В данной работе рассматриваются только итерационные алгоритмы шифрования с независимыми и равновероятно выбираемыми раундовыми ключами. Заметим, что разностный метод и его обобщения часто применяются в марковской модели для таких алгоритмов блочного шифрования.

О п р е д е л е н и е 2 ([2]). Итерационный алгоритм блочного шифрования с раундовой функцией i-го раунда $g^{(i)}$ и с независимыми и равновероятно выбираемыми раундовыми ключами называется $\otimes$-*марковским*, если для всех элементов $\theta, \varepsilon \in X^{\times}$, $\alpha \in X$ и $i \in \{1, \ldots, l\}$ выполняется равенство

$$p_{\theta,\,\varepsilon}(g^{(i)}\,|\,\alpha) = p_{\theta,\,\varepsilon}(g^{(i)}), \tag{1}$$

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

Итерационные $\otimes$-марковские алгоритмы блочного шифрования обладают следующим свойством.

Теорема 1 ([2]). *Пусть $(X, \otimes)$ — абелева группа, $\xi^{(0)}$ — дискретная случайная величина со значениями в множестве X. Тогда в l-раундовом итерационном $\otimes$-марковском алгоритме блочного шифрования с независимыми и равновероятно выбираемыми раундовыми ключами раундовые разности $\xi^{(t)} = (\xi^{(0)} \otimes \alpha)^{f_{\vec{k}_t}} \overline{\otimes} \alpha^{f_{\vec{k}_t}}$, являясь случайными величинами, образуют цепь Маркова.*

Из теоремы 1 следует, что для всех $t \in \mathbb{N}$ и $\theta^{(t,\ldots,0)} = (\theta^{(t)}, \ldots, \theta^{(0)}) \in (X^{\times})^{t+1}$ выполняется равенство

$$\mathbf{P}\{\xi^{(t,\ldots,0)} = \theta^{(t,\ldots,0)}\} = \mathbf{P}\{\xi^{(0)} = \theta^{(0)}\} \prod_{i=0}^{t-1} p_{\,\theta^{(i)},\,\theta^{(i+1)}}(g). \tag{2}$$

Известен следующий класс $\otimes$-марковских алгоритмов блочного шифрования.

Утверждение 1 ([15]). *Пусть $(X, \otimes)$ — абелева группа, $X' \subseteq X$, $|X'| \geqslant 0$, $k = (k_1, k_2) \in X \times X'$, $v_{k_2} \in S(X)$ и частичная раундовая функция $g_k \in S(X)$ задана условием $g_k : \alpha \mapsto (\alpha \otimes k_1)^{v_{k_2}}$. Тогда итерационный алгоритм шифрования с раундовой функцией g и независимыми и равновероятно выбираемыми раундовыми ключами является $\otimes$-марковским.*

3. Цепи Маркова на W-разбиениях

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

$$\zeta^{(t)} \in U_j \quad \text{для каждого} \quad j \in \{0, \ldots, r-1\}, \;\; t = 1, \ldots, l.$$

О п р е д е л е н и е 3 ([3]). 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 $\zeta_{\mathbf{U}}^{(0)}$, $\zeta_{\mathbf{U}}^{(1)}, \ldots, \zeta_{\mathbf{U}}^{(l)}$ является цепью Маркова, переходные вероятности которой не зависят от распределения случайной величины $\zeta^{(0)}$. Полученную цепь Маркова будем называть *укрупненной*.

Укрупненная марковская цепь $\zeta_{\mathbf{U}}^{(0)}, \zeta_{\mathbf{U}}^{(1)}, \ldots, \zeta_{\mathbf{U}}^{(l)}$ может допускать дальнейшее укрупнение. В связи с этим введем следующее определение.

О п р е д е л е н и е 4. Пусть Y — произвольное конечное множество. Объединением разбиения $\mathbf{W} = \{W_0, \ldots, W_{d-1}\}$ множества Y называется разбиение $\mathbf{W}' = \{W'_0, \ldots, W'_{d'-1}\}$, блоки которого являются объединением блоков разбиения $\mathbf{W}$, т. е. $W'_c = \bigcup_{i \in J_c} W_i$ для некоторого разбиения $J = \{J_0, \ldots, J_{d'-1}\}$ множества $\{0, \ldots, d-1\}$. Для $\mathbf{U} = \{U_0, \ldots, U_{r-1}\}$ и $t = 1, \ldots, l$ положим

$$p_{\theta, U_c} = \sum_{\theta' \in U_c} q_{\theta, \theta'}, \quad \theta \in Q, \ c \in \{0, \ldots, r-1\}.$$

Из теоремы 6.3.2 в [3] следует критерий того, что последовательность случайных величин $\zeta_{\mathbf{U}}^{(0)}$, $\zeta_{\mathbf{U}}^{(1)}, \ldots, \zeta_{\mathbf{U}}^{(l)}$ является укрупненной цепью Маркова.

Утверждение 2 ([3]). *Тогда и только тогда состояния марковской последовательности случайных величин $\zeta^{(0)}, \zeta^{(1)}, \ldots, \zeta^{(l)}$ допускают укрупнение посредством разбиения $\mathbf{U} = \{U_0, \ldots, U_{r-1}\}$, $r \geqslant 2$, когда выполняется равенство $p_{\theta, U_c} = a_{j,c}$ для каждых $(j, c) \in \{0, \ldots, r-1\}^2$ $\theta \in U_j$ и некоторых $a_{j,c}$, $0 \leqslant a_{j,c} \leqslant 1$.*

Очевидно, что итерационному алгоритму блочного шифрования с раундовой функцией g и независимыми и равновероятно выбираемыми раундовыми ключами соответствует цепь Маркова $\xi^{(0,2)}, \xi^{(1,2)}, \ldots, \xi^{(l,2)}$ с множеством состояний X^2 и матрицей вероятностей переходов $(p_{\alpha, \alpha'}^{(1,2)}(g))$, элементы которой заданы условием

$$p_{\alpha, \alpha'}^{(1,2)}(g) = \mathbf{P}\{(\alpha_1^{g_k}, \alpha_0^{g_k}) = \alpha'\},$$

где $g : X \times K \to X$, $k \in_U K$, $\alpha = (\alpha_1, \alpha_0) \in X^2$, $\alpha' \in X^2$.

Покажем, что определение 2, а также теорема 1 и утверждение 1 непосредственно следуют из условий, при которых возможно укрупнение состояний цепи Маркова $\xi^{(0,2)}, \xi^{(1,2)}, \ldots, \xi^{(l,2)}$.

Рассмотрим разбиение $\mathbf{X} = \{ X_\varepsilon | \varepsilon \in X\}$ множества X^2 с блоками

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

Заметим, что если $k \in_U K$, то для всех $\alpha, \varepsilon, \theta \in X$ справедливо равенство

$$\begin{aligned} p_{(\theta\otimes\alpha,\,\alpha),\,X_\delta}(g) &= \mathbf{P}\big\{((\theta \otimes \alpha)^{g_k}, \alpha^{g_k}) \in X_\varepsilon\big\} = \\ &= \mathbf{P}\big\{(\theta \otimes \alpha)^{g_k} \overline{\otimes} \alpha^{g_k} = \varepsilon\big\} = p_{\theta,\,\varepsilon}(g\,|\,\alpha). \end{aligned} \tag{3}$$

Из утверждения 2 следует, что марковская последовательность $\xi^{(0,2)}, \xi^{(1,2)}, \ldots, \xi^{(l,2)}$ допускает укрупнение посредством разбиения $\mathbf{X}$, если для всех $\alpha, \beta, \varepsilon, \theta \in X$ выполняется равенство

$$p_{(\theta\otimes\alpha,\,\alpha),\,X_\varepsilon}(g) = p_{(\theta\otimes\beta,\beta),\,X_\varepsilon}(g). \tag{4}$$

Из равенств (3), (4) вытекает условие

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

на котором основано определение 2 $\otimes$-марковского алгоритма блочного шифрования. Кроме того, из утверждения 2 непосредственно следует теорема 1. Тем самым последовательность $\xi_{\mathbf{X}}^{(0,2)}, \xi_{\mathbf{X}}^{(1,2)}, \ldots, \xi_{\mathbf{X}}^{(l,2)}$ является цепью Маркова.

Далее нас будут интересовать укрупнения цепи $\xi_{\mathbf{X}}^{(0,2)}, \xi_{\mathbf{X}}^{(1,2)}, \ldots, \xi_{\mathbf{X}}^{(l,2)}$, при которых сохраняется марковость. Для удобства дальнейших обозначений положим

$$\xi^{(0)} = \xi_{\mathbf{X}}^{(0,2)}, \;\; \xi^{(1)} = \xi_{\mathbf{X}}^{(1,2)}, \;\ldots,\; \xi^{(l)} = \xi_{\mathbf{X}}^{(l,2)}.$$

В данном разделе будем рассматривать произвольный $\otimes$-марковский итерационный l-раундовый алгоритм блочного шифрования с раундовой функцией g и независимыми и равновероятно выбираемыми раундовыми ключами. Для такого алгоритма шифрования и любой дискретной случайной величины $\xi^{(0)}$ на множестве X последовательность случайных величин

$$\xi^{(t)} \;=\; (\xi^{(0)} \otimes \alpha)^{f_{\vec{k}_t}} \overline{\otimes} \alpha^{f_{\vec{k}_t}}, \quad t = 1, \ldots, l,$$

является цепью Маркова для каждого $\alpha \in X$.

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

$$\mathbf{W} \notin \big\{\{\alpha\} \,\big|\, \alpha \in X\},\; \{X\}\big\}.$$

Заметим, что для произвольного $\otimes$-марковского алгоритма шифрования для всех $t \in \{1,\dots,l\}$, $j^{(t,\dots,0)} = (j^{(t)},\dots,j^{(0)}) \in \{0,\dots,r-1\}^{t+1}$ справедливо равенство

$$\begin{aligned}
&\mathbf{P}\{\xi_{\mathbf{W}}^{(t,\dots,0)} = j^{(t,\dots,0)}\} = \\
&= \sum_{(\theta^{(t)},\dots,\theta^{(0)})\in W_{j^{(t)}}\times\cdots\times W_{j^{(0)}}} \mathbf{P}\{\xi^{(t,\dots,0)} = (\theta^{(t)},\dots,\theta^{(0)})\} = \\
&= \sum_{(\theta^{(t)},\dots,\theta^{(0)})\in W_{j^{(t)}}\times\cdots\times W_{j^{(0)}}} \mathbf{P}\{\xi^{(0)} = \theta^{(0)}\} \times \\
&\qquad \times \mathbf{P}\{\xi^{(1)} = \theta^{(1)} \mid \xi^{(0)} = \theta^{(0)}\} \times \\
&\qquad \times \mathbf{P}\{\xi^{(2)} = \theta^{(2)} \mid \xi^{(1,0)} = \theta^{(1,0)}\} \times \cdots \\
&\qquad \cdots \times \mathbf{P}\{\xi^{(t)} = \theta^{(t)} \mid \xi^{(t-1,\dots,0)} = \theta^{(t-1,\dots,0)}\} = \\
&= \sum_{\theta^{(0)}\in W_{j^{(0)}}} \mathbf{P}\{\xi^{(0)} = \theta^{(0)}\} \sum_{\theta^{(1)}\in W_{j^{(1)}}} p_{\theta^{(0)},\theta^{(1)}}(g^{(1)}) \sum_{\theta^{(2)}\in W_{j^{(2)}}} p_{\theta^{(1)},\theta^{(2)}}(g^{(2)}) \times \cdots \\
&\qquad \cdots \times \sum_{\theta^{(t-1)}\in W_{j^{(t-1)}}} p_{\theta^{(t-2)},\theta^{(t-1)}}(g^{(t-1)}) \sum_{\theta^{(t)}\in W_{j^{(t)}}} p_{\theta^{(t-1)},\theta^{(t)}}(g^{(t)}). \quad (5)
\end{aligned}$$

Равенство (5) облегчает получение вероятности $\mathbf{P}\{\xi_{\mathbf{W}}^{(t,\dots,0)} = j^{(t,\dots,0)}\}$ для $\otimes$-марковских алгоритмов шифрования. Для ее нахождения сначала вычисляется для $\theta^{(t-1)} \in W_{j^{(t-1)}}$ вероятность

$$p^{[1]}_{\theta^{(t-1)},W_{j^{(t)}}}(g^{(t)}) = p_{\theta^{(t-1)},W_{j^{(t)}}}(g^{(t)}) = \sum_{\theta^{(t)}\in W_{j^{(t)}}} p_{\theta^{(t-1)},\theta^{(t)}}(g^{(t)}).$$

Затем для $i = 2,\dots,t$ и каждого $\theta^{(t-i)} \in W_{j^{(t-i)}}$ рекурсивно находятся вероятности

$$\begin{aligned}
&p^{[i]}_{\theta^{(t-i)},j^{(t)},\dots,j^{(t-i+1)}}\big(g^{(t)},\dots,g^{(t-i+1)}\big) = \\
&= \sum_{\theta^{(t-i+1)}\in W_{j^{(t-i+1)}}} p_{\theta^{(t-i)},\,\theta^{(t-i+1)}}\big(g^{(t-i+1)}\big)\, p^{[i-1]}_{\theta^{(t-i+1)},\,j^{(t-i+2)}}\big(g^{(t-i+2)}\big). \quad (6)
\end{aligned}$$

Заметим, что для $\otimes$-марковских алгоритмов шифрования равенство (6) для разбиения $\mathbf{W}$ является аналогом равенства (2).

Далее рассматриваются разбиения $\mathbf{W}$ множества X, для которых последовательность $\xi^{(0)}_{\mathbf{W}}, \ldots, \xi^{(l)}_{\mathbf{W}}$ образует цепь Маркова. Отметим, что

$$p_{\theta,W_c}(g^{(t)}) = \sum_{\theta' \in W_c} p_{\theta,\theta'}(g^{(t)}), \theta \in X, c \in \{0, \ldots, r-1\},$$

для $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$ и $t = 1, \ldots, l$.

Из утверждения 2 следует критерий того, что последовательность случайных величин $\xi^{(0)}_{\mathbf{W}}, \ldots, \xi^{(l)}_{\mathbf{W}}$ является укрупненной цепью Маркова для $\otimes$-марковского алгоритма блочного шифрования.

Утверждение 3. *Тогда и только тогда для итерационного l-раундового $\otimes$-марковского алгоритма блочного шифрования с раундовой функцией t-го раунда $g^{(t)}$ состояния марковской последовательности случайных величин $\xi^{(0)}, \ldots, \xi^{(l)}$ допускают укрупнение посредством разбиения $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$, $r \geqslant 2$, когда для каждых $(j,c) \in \{0, \ldots, r-1\}^2$, $(\theta, t) \in W_j \times \{1, \ldots, l\}$ и некоторых $a^{(t)}_{j,c}$, $0 \leqslant a^{(t)}_{j,c} \leqslant 1$, выполняется равенство*

$$p_{\theta,W_c}(g^{(t)}) = a^{(t)}_{j,c}.$$

Если $g^{(1)} = g^{(2)} = \cdots = g^{(l)}$, то укрупненная цепь Маркова является однородной.

Доказательство следует из теоремы 6.3.2 в [3] и того, что если $g^{(1)} = g^{(2)} = \cdots = g^{(l)}$, то для всех $t \in \{2, \ldots, l\}$, $\theta \in W_j$, $j, c \in \{0, \ldots, r-1\}$

$$\mathbf{P}\{\xi^{(t)}_{\mathbf{W}} = c \mid \xi^{(t-1)}_{\mathbf{W}} = j\} = p_{\theta,W_c}(g^{(t)}),$$

т. е. $\xi^{(0)}_{\mathbf{W}}, \ldots, \xi^{(l)}_{\mathbf{W}}$ — однородная цепь Маркова. □

Пусть разбиение $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$ таково, что для каждых $(c,j) \in \{0, \ldots, r-1\}^2$, $(\theta, t) \in W_j \times \{1, \ldots, l\}$ и некоторых $a^{(t)}_{j,c}$, $0 \leqslant a^{(t)}_{j,c} \leqslant 1$, выполняется условие

$$p_{\theta,W_c}(g^{(t)}) = a^{(t)}_{j,c}.$$

Тогда из равенства (5) и утверждения 3 следует марковость цепи $\xi^{(0)}_{\mathbf{W}}, \ldots, \xi^{(l)}_{\mathbf{W}}$ для каждого начального распределения случайной величины $\xi^{(0)}$. Однако для некоторых цепей Маркова существуют начальные распределения $\xi^{(0)}$, не удовлетворяющие данному условию и такие, что $\xi^{(0)}_{\mathbf{W}}, \ldots, \xi^{(l)}_{\mathbf{W}}$ — также цепь Маркова для разбиения $\mathbf{W}$. В этом случае говорим, что цепь Маркова $\xi^{(0)}, \ldots, \xi^{(l)}$ допускает *слабое укрупнение* посредством разбиения $\mathbf{W}$.

Из утверждения 3 также следует, что если для каждых $t \in \{1,\dots,l\}$, $(j,c) \in \{0,\dots,r-1\}^2$, $(\theta,\theta') \in W_j \times W_c$ и некоторых $a_{j,c}^{(t)}$, $0 \leqslant a_{j,c}^{(t)} \leqslant 1$,

$$p_{\theta,\theta'}(g^{(t)}) = a_{j,c}^{(t)},$$

то $\xi_{\mathbf{W}}^{(0)},\dots,\xi_{\mathbf{W}}^{(l)}$ — укрупненная цепь Маркова для разбиения $\mathbf{W} = \{W_0,\dots,W_{r-1}\}$.

О п р е д е л е н и е 5. Назовем l-раундовый итерационный $\otimes$-марковский алгоритм блочного шифрования с марковской последовательностью $\xi^{(0)},\dots,\xi^{(l)}$ (*слабо*) $\otimes_{\mathbf{W}}$-*марковским* для разбиения $\mathbf{W} = \{W_0,\dots,W_{r-1}\}$, $r \geqslant 2$, если последовательность случайных величин $\xi_{\mathbf{W}}^{(0)},\dots,\xi_{\mathbf{W}}^{(l)}$ является цепью Маркова (при некотором распределении случайной величины ξ_0).

В случае $\otimes_{\mathbf{W}}$-марковости алгоритма блочного шифрования получаем, что для каждых $(j,c) \in \{0,\dots,r-1\}^2$, $(\theta,t) \in W_j \times \{1,\dots,l\}$ и некоторых $a_{j,c}^{(t)}$, $0 \leqslant a_{j,c}^{(t)} \leqslant 1$, имеет место равенство

$$p_{\theta,W_c}(g^{(t)}) = a_{j,c}^{(t)}.$$

Поэтому раундовой функции $g^{(t)}$ на t-м раунде $\otimes_{\mathbf{W}}$-марковского алгоритма блочного шифрования поставим в соответствие матрицу

$$\mathbf{p}_{\mathbf{W}}(g^{(t)}) = \bigl(p_{W_j,W_c}(g^{(t)})\bigr)$$

вероятностей переходов блоков, где

$$p_{W_j,W_c}(g^{(t)}) = a_{j,c}^{(t)} \quad \text{для} \quad (j,c) \in \{0,\dots,r-1\}^2,\ t = 1,\dots,l.$$

Тогда для l-раундовой функции зашифрования $f^{(l)}$ матрица $(p_{W_i,W_j}(f^{(l)}))$ вероятностей переходов блоков разбиения $\mathbf{W}$ равна $\prod_{i=1}^{l} \mathbf{p}_{\mathbf{W}}(g^{(i)})$.

В XSL-алгоритмах блочного шифрования и алгоритмах шифрования Фейстеля с XSL-функцией усложнения (т. е. являющейся композицией наложения раундового ключа, S-бокса и линейного преобразования) $\otimes_{\mathbf{W}}$-марковость последовательности случайных величин $\xi_{\mathbf{W}}^{(0)},\dots,\xi_{\mathbf{W}}^{(l)}$ определяется свойствами преобразований слоя S-боксов и линейного слоя. В связи с этим введем понятие $\otimes_{\mathbf{W}}$-марковского преобразования, следующее из определения 5.

Рассмотрим матрицу вероятностей переходов разностей $\widehat{\mathbf{p}}(b) = (\widehat{p}_{\theta,\varepsilon}(b))$ преобразования $b \in S(X)$, элементы которой заданы условием

$$\widehat{p}_{\theta,\varepsilon}(b) = \frac{1}{|X|}\left|\left\{\alpha \in X \middle| (\theta \otimes \alpha)^b = \varepsilon \otimes \alpha^b\right\}\right|, \quad \theta, \varepsilon \in X.$$

В отличие от соответствующей вероятности $p_{\theta,\varepsilon}(g^{(i)})$ переходов раундовой функции здесь нет усреднения по раундовым ключам. Заметим, что для многих алгоритмов блочного шифрования вероятность $p_{\theta,\varepsilon}(g^{(i)})$ однозначно определяется через вероятности переходов разностей преобразований, составляющих раундовую функцию. Так, из утверждения 1 следует $\otimes$-марковость итерационного алгоритма блочного шифрования с раундовой функцией $b' : X^2 \to X$, заданной через частичные функции условием

$$b'_k : \alpha \mapsto (\alpha \otimes k)^b \quad \text{для каждого} \quad k \in X.$$

Отсюда вытекает равенство

$$\widehat{p}_{\theta,\varepsilon}(b) = p_{\theta,\varepsilon}(b') \quad \text{для всех} \quad \theta, \varepsilon \in X.$$

При $(X, \otimes) = (V_n, \oplus)$ для XSL-алгоритмов блочного шифрования выполняется равенство $b = sh$, $s = (s_{d-1}, \ldots, s_0)$ — преобразование нелинейного слоя, $n = md$, h — преобразование линейного слоя, $s \in (S(V_m))^d$, $h \in GL_n$. Кроме того, для всех $\theta, \varepsilon \in V_n$ справедливы равенства

$$p_{\theta,\varepsilon}(b') = \widehat{p}_{\theta,\varepsilon}(b) = \widehat{p}_{\theta,\varepsilon}(sh) = \widehat{p}_{\theta,\varepsilon^{h^{-1}}}(s) = p_{\theta,\varepsilon^{h^{-1}}}(s') =$$
$$= \prod_{i=0}^{d-1} p_{\theta_i,\varepsilon'_i}(s'_i) = \prod_{i=0}^{d-1} \widehat{p}_{\theta_i,\varepsilon'_i}(s_i),$$

где $\varepsilon' = \varepsilon^h = (\varepsilon'_{d-1}, \ldots, \varepsilon'_0)$, а отображения $s' : V_n^2 \to V_n$, $s'_i : V_m^2 \to V_m$ заданы условиями

$$s'_i : \alpha_i \mapsto (\alpha_i \oplus k_i)^{s_i}, \quad s' : \alpha \mapsto (\alpha \oplus k)^s$$

для всех $k = (k_{d-1}, \ldots, k_0) \in V_m^d$, $\alpha = (\alpha_{d-1}, \ldots, \alpha_0) \in V_m^d$, $i \in \{0, \ldots, d-1\}$.

Для преобразования $b \in S(X)$ положим

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

О п р е д е л е н и е 6. Преобразование $b \in S(X)$ назовем $\otimes_{\mathbf{W}}$-*марковским* для разбиения $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$, $|X| \geqslant r \geqslant 2$, если

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

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

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

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

для каждых $(j, c) \in \{0, \ldots, r-1\}^2$, $\theta \in W_j$ и некоторых $a_{j,c}$, $0 \leqslant a_{j,c} \leqslant 1$. При этом матрица $\mathbf{p}_{\mathbf{W}}(g)$ однозначно выражается через матрицу $\widehat{\mathbf{p}}(s)$. Кроме того, для XSL-алгоритмов блочного шифрования матрицы $\mathbf{p}(g)$, $\widehat{\mathbf{p}}(s)$ различаются только перестановками строк и столбцов. В свою очередь, для S-бокса $(s_{d-1}, \ldots, s_0)$, заданного подстановками $s_0, \ldots, s_{d-1} \in S(V_m)$, матрица $\widehat{\mathbf{p}}(s)$ есть тензорное произведение матриц $\widehat{\mathbf{p}}(s_0), \ldots, \widehat{\mathbf{p}}(s_{d-1})$. Отсюда следует, что для разбиения $\mathbf{W} = \mathbf{W}_{d-1} \times \cdots \times \mathbf{W}_0$ матрица $\widehat{\mathbf{p}}_{\mathbf{W}}(s)$ также является тензорным произведением матриц $\widehat{\mathbf{p}}_{\mathbf{W}_0}(s_0), \ldots, \widehat{\mathbf{p}}_{\mathbf{W}_{d-1}}(s_{d-1})$, где $\mathbf{W}_i$ — произвольное разбиение пространства V_m для $i = 0, \ldots, d-1$. Поэтому часто свойство $\otimes_{\mathbf{W}}$-марковости алгоритма следует из марковости преобразования, которое может доказываться существенно проще. Классы $\otimes_{\mathbf{W}}$-марковских преобразований будут рассмотрены далее в разделах 4, 5, 6.

Для $t \in \{1, \ldots, l\}$ и произвольных подмножеств U, U' множества X положим

$$p_{U,U'}(g^{(t)}) = \frac{\left|\left\{(\alpha, k^{(t)}, \theta) \in X \times K^{(t)} \times U \middle| (\theta \otimes \alpha)^{g_{k^{(t)}}(t)} \overline{\otimes} \alpha^{g_{k^{(t)}}(t)} \in U'\right\}\right|}{|K^{(t)}||X||U|}.$$

Для l-раундового итерационного $\otimes_{\mathbf{W}}$-марковского алгоритма шифрования

$$p_{W_{j^{(0)}}, W_{j^{(l)}}}(f^{(l)}) = \sum_{j^{(1)} \in \{0, \ldots, r-1\}} \cdots \sum_{j^{(l-1)} \in \{0, \ldots, r-1\}} \prod_{i=1}^{l} p_{W_{j^{(i-1)}}, W_{j^{(i)}}}(g^{(i)}), \quad (7)$$

а для $t \in \{1, \ldots, l\}$, $j^{(t, \ldots, 0)} = (j^{(t)}, \ldots, j^{(0)}) \in \{0, \ldots, r-1\}^{t+1}$ справедливо равенство

$$\mathbf{P}\left\{\xi_{\mathbf{W}}^{(t, \ldots, 1)} = j^{(t, \ldots, 1)} \middle| \xi_{\mathbf{W}}^{(0)} = j^{(0)}\right\} = \prod_{i=0}^{t-1} p_{W_{j^{(i)}}, W_{j^{(i+1)}}}(g^{(i+1)}). \quad (8)$$

Отметим, что равенство (7) выполняется, если $\xi^{(0)}_{\mathbf{W}}, \ldots, \xi^{(l)}_{\mathbf{W}}$ — укрупненная цепь Маркова. Однако аналог равенства (8) может быть справедливым и в случае алгоритма, не являющегося $\otimes_{\mathbf{W}}$-марковским. Для $\otimes$-марковского алгоритма блочного шифрования приведем условия на подмножества множества X, при которых возможны аналоги равенства (8). Так, из равенства (5) следует, что если только часть подблоков разбиения $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$ для некоторого подмножества $J \subseteq \{0, \ldots, r-1\}$ удовлетворяет условию

$$p_{\theta, W_c}(g^{(t)}) = a^{(t)}_{j,c}$$

для каждых $(j, c) \in J^2$, $(\theta, t) \in W_j \times \{1, \ldots, l\}$ и некоторых $a^{(t)}_{j,c}$, $0 \leqslant a^{(t)}_{j,c} \leqslant 1$, то справедливо равенство (8) для каждого набора $j^{(t,\ldots,0)} \in J^{t+1}$. Это оправдывает введение следующего понятия.

О п р е д е л е н и е 7. Назовем l-раундовый итерационный $\otimes$-марковский алгоритм блочного шифрования (преобразование $b \in S(X)$) $\otimes^{(J)}_{\mathbf{W}}$-*марковским* для разбиения $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$ и непустого подмножества $J \subseteq \{0, \ldots, r-1\}$, если

$$p_{\theta, W_{j_2}}(g^{(t)}) = a^{(t)}_{j_1, j_2} \quad (\widehat{p}_{\theta, W_{j_2}}(b) = a_{j_1, j_2})$$

для каждых $t \in \{1, \ldots, t\}$, $j_1, j_2 \in J$, $\theta \in W_{j_1}$ и некоторых $a^{(t)}_{j_1, j_2}$, $0 \leqslant a^{(t)}_{j_1, j_2} \leqslant 1$ (a_{j_1, j_2}, $0 \leqslant a_{j_1, j_2} \leqslant 1$).

Из утверждения 3 следует, что $\otimes^{(J)}_{\mathbf{W}}$-марковский алгоритм блочного шифрования (преобразование) является $\otimes_{\mathbf{W}}$-марковским при $J = \{0, \ldots, r-1\}$.

Для $\otimes^{(J)}_{\mathbf{W}}$-марковского алгоритма блочного шифрования вместо матрицы $\mathbf{p}_{\mathbf{W}}(g^{(t)})$ рассматривается $(d_J \times d_J)$-матрица

$$\mathbf{p}^{(J)}_{\mathbf{W}}(g^{(t)}) = (p^{(J)}_{W_{j_c}, W_{j_m}}(g^{(t)})), \quad t = 1, \ldots, l,$$

где $d_J = |J|$, $J = \{j_1, \ldots, j_{d_J}\}$, $j_1 < j_2 < \ldots < j_{d_J}$. Тогда элементы матрицы

$$\mathbf{p}^{(J)}_{\mathbf{W}}(g^{(1)}) \cdots \mathbf{p}^{(J)}_{\mathbf{W}}(g^{(l)}) = (p^{(J,l)}_{W_{j_c}, W_{j_m}})$$

удовлетворяют неравенству $p^{(l)}_{W_{j_c}, W_{j_m}} \geqslant p^{(J,l)}_{W_{j_c}, W_{j_m}}$, т. е. вероятность $p^{(J,l)}_{W_{j_c}, W_{j_m}}$ является оценкой снизу вероятности $p^{(l)}_{W_{j_c}, W_{j_m}}$ и справедливо равенство

$$p^{(l)}_{W_{j^{(0)}}, W_{j^{(l)}}} = \sum_{j^{(1)} \in J} \cdots \sum_{j^{(l-1)} \in J} \prod_{i=1}^{l} p_{W_{j^{(i-1)}}, W_{j^{(i)}}}(g^{(i)}), \quad (j^{(0)}, j^{(l)}) = (j_c, j_m).$$

Тем самым для алгоритма блочного шифрования, который не является $\otimes_{\mathbf{W}}$-марковским, но является $\otimes_{\mathbf{W}}^{(J)}$-марковским, с помощью равенства (8) находится вероятность

$$\mathbf{P}\{\xi_{\mathbf{W}}^{(t,\ldots,1)} = j^{(t,\ldots,1)} | \xi_{\mathbf{W}}^{(0)} = j^{(0)}\} \quad \text{при} \quad j^{(t,\ldots,0)} \in J^{t+1},$$

а также оценка снизу вероятности $p_{W_{j_c},W_{j_m}}^{(J,l)}$.

Аналог равенства (8) получается также при рассмотрении некоторых упорядоченных наборов подмножеств множества X, а условия, которые на них накладываются, содержатся в следующем определении.

О п р е д е л е н и е 8. Назовем l-раундовый итерационный $\otimes$-марковский алгоритм $\otimes_{\vec{U}}$-*марковским*, если упорядоченный набор $\vec{U} = (U_{j^{(l)}}, \ldots, U_{j^{(0)}})$ подмножеств множества X таков, что

$$p_{\theta,U_{j^{(t)}}}(g^{(t)}) = a_{j^{(t-1)},j^{(t)}}^{(t)}$$

для каждых $t \in \{1,\ldots,l\}$, $\theta \in U_{j^{(t-1)}}$ и некоторых $a_{j^{(t-1)},j^{(t)}}^{(t)}$, $0 \leqslant a_{j^{(t-1)},j^{(t)}}^{(t)} \leqslant 1$.

Из равенства (7) следует, что для каждых упорядоченного набора $\vec{U} = (U_{j^{(l)}}, \ldots, U_{j^{(0)}})$ и $\otimes_{\vec{U}}$-марковского алгоритма шифрования имеем

$$\begin{aligned} &\mathbf{P}\{(U_{j^{(t)}}, \ldots, U_{j^{(0)}})\} = \\ &= \mathbf{P}\{\xi^{(t,\ldots,1)} \in U_{j^{(t)}} \times \ldots \times U_{j^{(1)}} | \xi^{(0)} \in U_{j^{(0)}}\} = \\ &= \prod_{i=0}^{t-1} p_{U_{j^{(i)}},U_{j^{(i+1)}}}(g^{(i+1)}). \end{aligned} \tag{9}$$

Равенство (9) является аналогом равенства (8). Кроме того, если у $\otimes_{\vec{U}}$-марковского алгоритма $U_{j^{(0)}}, \ldots, U_{j^{(l)}}$ — блоки некоторого разбиения $\mathbf{W}$, то равенства (8), (9) совпадают. Ясно, что любой $\otimes_{\mathbf{W}}$-марковский алгоритм блочного шифрования является $\otimes_{\vec{U}}$-марковским для каждого набора $\vec{U}$ блоков $U_{j^{(0)}}, \ldots, U_{j^{(l)}}$ разбиения $\mathbf{W}$. Неявно допущение о $\otimes_{\vec{U}}$-марковости алгоритма блочного шифрования для некоторого класса упорядоченных наборов используется в методе усеченных разностей (см. [8, 9]).

О п р е д е л е н и е 9. *Усеченной разностью* называется такое подмножество

$$\{(\theta_{m-1},\dots,\theta_0)\in Y^m \,|\, \theta_{i_1}=\widetilde{0},\dots,\theta_{i_c}=\widetilde{0}\},\quad 0\leqslant i_1<\dots<i_c\leqslant m-1,$$

множества X, что $X=Y^m$ для некоторой аддитивной абелевой группы Y с нулевым элементом $\widetilde{0}$ и некоторого числа $m\in\mathbb{N}$. Разбиение $\mathbf{W}$, блоком которого является усеченная разность, назовем *усеченным*.

В методе усеченных разностей (см. [8 – 13]) используется следующее предположение, которое является частным случаем $\otimes_{\vec{U}}$-марковости алгоритма шифрования.

Предположение 1. *Пусть* $(A_{j^{(l)}},\dots,A_{j^{(0)}})$ *— набор усеченных разностей, где* $A_{j^{(0)}},\dots,A_{j^{(l)}}$ *— подмножества множества* X. *Тогда для каждых* $t\in\{1,\dots,l\}$, $(\theta,\theta')\in A_{j^{(t-1)}}\times A_{j^{(t)}}$ *и некоторых* $a^{(t)}_{j^{(t-1)},j^{(t)}}$, $0\leqslant a^{(t)}_{j^{(t-1)},j^{(t)}}\leqslant 1$, *справедливо равенство*

$$p_{\theta,\theta'}(g^{(t)})=a^{(t)}_{j^{(t-1)},j^{(t)}}.$$

Для итерационных $\otimes$-марковских алгоритмов шифрования, имея в виду предположение 1, неявно считают, что вероятность $\mathbf{P}\{(A_{j^{(l)}},\dots,A_{j^{(0)}})\}$ набора усеченных разностей $(A_{j^{(l)}},\dots,A_{j^{(0)}})$, называемого *усеченной разностной характеристикой*, находится с помощью равенства (9). При применении метода усеченных разностей в ряде работ (см., например, [10, 12]) проверяется корректность предположения 1 сравнением оценок вероятности $\mathbf{P}\{(A_{j^{(l)}},\dots,A_{j^{(0)}})\}$, найденных для небольшого числа раундов l двумя способами. В первом случае осуществляется вычислительный эксперимент, во втором применяется формула (9). Так, в [12] показано, что экспериментальная оценка вероятности $\mathbf{P}\{(A_{j^{(l)}},\dots,A_{j^{(0)}})\}$ может быть больше найденной по формуле (9). Заметим, что если набор $\vec{A}=(A_{j^{(l)}},\dots,A_{j^{(0)}})$ усеченных разностей удовлетворяет предположению 1, т. е. $p_{\theta,\theta'}(g^{(t)})=a^{(t)}_{j^{(t-1)},j^{(t)}}$ для каждых $t\in\{1,\dots,l\}$, $(\theta,\theta')\in A_{j^{(t-1)}}\times A_{j^{(t)}}$ и некоторых $a^{(t)}_{j^{(t-1)},j^{(t)}}$, $0\leqslant a^{(t)}_{j^{(t-1)},j^{(t)}}\leqslant 1$, то отсюда следует $\otimes_{\vec{A}}$-марковость алгоритма шифрования. Поэтому условия, которым должен удовлетворять $\otimes_{\vec{U}}$-марковский алгоритм шифрования, являются более слабыми по сравнению с условиями предположения 1. Отметим, что для большинства алгоритмов блочного шифрования, для анализа которых применялся метод усеченных разностей, справедливость предположения 1 не проверялась.

Приведем условия на объединение $\mathbf{W}'$ разбиения $\mathbf{W}$ множества X, при которых из $\otimes_{\mathbf{W}}$-марковости раундовой функции g для разбиения $\mathbf{W}$ следует ее $\otimes_{\mathbf{W}'}$-марковость.

Утверждение 4. *Пусть раундовая функция $g: X \times K \to X$ является $\otimes_{\mathbf{W}}$-марковской для разбиения $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ множества X и $p_{\theta,W_j}(g) = a_{i,j}(g)$ для всех $i, j \in \{0, \dots, r-1\}$, $\theta \in W_i$. Функция g является $\otimes_{\mathbf{W}'}$-марковской, если объединение $\mathbf{W}' = \{W'_0, \dots, W'_{r'-1}\}$ разбиения $\mathbf{W}$ таково, что*:

1) $W'_c = \bigcup_{i \in J_c} W_i$ *для некоторого разбиения* $J = \{J_0, \dots, J_{r'-1}\}$ *множества* $\{0, \dots, r-1\}$ *при* $c = 0, \dots, r'-1$,
2) $\sum_{j \in J_q} a_{c,j}(g) = \sum_{j \in J_q} a_{c',j}(g)$ *для каждых* $t, q \in \{0, \dots, r'-1\}$, $c, c' \in J_t$.

Доказательство следует из утверждения 3. □

Из утверждения 4 следует, что если раундовая функция $g : X \times K \to X$ является $\otimes^{(J)}_{\mathbf{W}}$-марковской для разбиения $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ и подмножества $J \subseteq \{0, \dots, r-1\}$, то она будет $\otimes^{(J')}_{\mathbf{W}'}$-марковской для укрупнения $\mathbf{W}' = \{W'_0, \dots, W'_{r'-1}\}$ разбиения $\mathbf{W}$ и подмножества $J' \subseteq \{0, \dots, r'-1\}$, если существует разбиение $\mathbf{U} = \{U_1, \dots, U_q\}$ множества J, удовлетворяющее следующим условиям:

1) $W'_j = \bigcup_{i \in U_j} W_i$ для каждого $j \in \{1, \dots, q\}$,
2) $\sum_{j \in U_q} a_{c,j}(g) = \sum_{j \in U_q} a_{c',j}(g)$ для каждых $t, q \in J'$, $c, c' \in U_t$, где $p_{\theta,W_j}(g) = a_{i,j}(g)$ при $i, j \in J$, $\theta \in W_i$.

4. $\otimes_{\mathbf{W}}$-марковость экспоненциальных подстановок

В данном разделе и следующих двух опишем разбиения $\mathbf{W}$, относительно которых подстановки S-боксов являются $\otimes_{\mathbf{W}}$-марковскими. Рассмотрим подстановки, основанные на операциях экспоненцирования и логарифмирования в кольце $\mathbb{Z}_n$ и поле $GF(n+1)$. Приведем для них разбиения $\mathbf{W}$, при которых они являются $+_{\mathbf{W}}$-марковскими.

Пусть $\mathbb{Z}$ — множество всех целых чисел, $Z_n = \{0, \dots, n-1\}$. Для $a \in \mathbb{Z}$ через $a_{(d)}$ обозначим такой наименьший элемент $a_{(d)} \in \{0, \dots, d-1\}$, что $a_{(d)} \equiv a \pmod d$. Пусть также $n \in \mathbb{N}$, $n+1$ — простое число, θ — примитивный элемент поля $GF(n+1)$, $\delta \in Z_n$, $c \in Z_n$, подстановка $\mu_{\theta,\delta,c} \in S(\mathbb{Z}_n)$ задана условием

$$\mu_{\theta,\delta,c} : x \mapsto (\theta^{x+c} (\mathrm{mod}\ n+1) + \delta)_{(n)}.$$

Отметим, что в алгоритме блочного шифрования SAFER [14] при $\delta = c = 0$, $n = 256$, $\theta = 45$ в S-боксе используются подстановки $\mu_{\theta,\delta,c}$, $\mu^{-1}_{\theta,\delta,c}$. Кроме того, S-боксом является преобразование, заданное на $\mathbb{Z}_{256}$ условием

$$x \mapsto \begin{cases} 45^x \pmod{257}, & \text{если} \quad 45^x \not\equiv 256 \pmod{257}, \\ 0, & \text{если} \quad 45^x \equiv 256 \pmod{257}. \end{cases}$$

Опишем свойства матрицы вероятностей переходов разностей подстановки $\mu_{\theta,\delta,c}$ при $n = 2^m$ для такого $m \in \mathbb{N}$, что $2^m + 1$ — простое число. Нетрудно убедиться, что для всех $a, b \in \mathbb{Z}$ выполняется равенство

$$(a_{(n+1)} - b_{(n+1)})_{(n)} = \begin{cases} (a - b)_{(n+1)}, & \text{если} \quad a_{(n+1)} \geqslant b_{(n+1)}, \\ (a - b)_{(n+1)} - 1, & \text{если} \quad a_{(n+1)} < b_{(n+1)}. \end{cases} \tag{10}$$

Для $\varepsilon \in Z_n^{\times}$ положим

$$\Lambda_{n,\theta,\varepsilon,c} = \left\{\alpha \in Z_n \middle| (\theta^{\alpha+c+\varepsilon})_{(n+1)} \geqslant (\theta^{\alpha+c})_{(n+1)}\right\},$$

$$\overline{\Lambda}_{n,\theta,\varepsilon,c} = Z_n \backslash \Lambda_{n,\theta,\varepsilon,c}.$$

Тогда из равенства (10) следует, что для каждых $\varepsilon \in Z_n^{\times}$, $\alpha \in Z_n$ выполняется равенство

$$\left(\mu_{\theta,\delta,c}(\alpha+\varepsilon) - \mu_{\theta,\delta,c}(\alpha)\right)_{(n)} =$$

$$= \begin{cases} \left(\theta^{\alpha+c}(\theta^{\varepsilon}-1)\right)_{(n+1)}, & \text{если} \quad \alpha \in \Lambda_{n,\theta,\varepsilon,c}, \\ \left(\theta^{\alpha+c}(\theta^{\varepsilon}-1)\right)_{(n+1)} - 1, & \text{если} \quad \alpha \in \overline{\Lambda}_{n,\theta,\varepsilon,c}. \end{cases} \tag{11}$$

Положим

$$\mathrm{E}_{n,\theta,\varepsilon,c} = \left\{(\theta^{\alpha+c}(\theta^{\varepsilon}-1))_{(n+1)} \middle| \, \alpha \in \Lambda_{n,\theta,\varepsilon,c}\right\},$$

$$\overline{\mathrm{E}}_{n,\theta,\varepsilon,c} = \left\{(\theta^{\alpha+c}(\theta^{\varepsilon}-1))_{(n+1)} - 1 \middle| \, \alpha \in \overline{\Lambda}_{n,\theta,\varepsilon,c}\right\}.$$

Заметим, что для каждых $\varepsilon \in Z_n^\times$, $\varepsilon' \in Z_{n+1}^\times$ существует такой единственный элемент $\alpha \in Z_n$, что

$$\theta^{\alpha+c+\varepsilon} - \theta^{\alpha+c} \equiv \varepsilon' \,(\mathrm{mod}\, n+1);$$

при этом

$$\alpha \equiv \log_\theta\bigl(\varepsilon'(\theta^{\varepsilon}-1)^{-1}\bigr) - c \,(\mathrm{mod}\, n),$$

где $\log_\theta(\varepsilon'(\theta^{\varepsilon}-1)^{-1})$ находится в поле $GF(n+1)$. Тогда из равенства (11) следует, что для каждых $\varepsilon, \lambda \in Z_n^\times$ справедливо равенство

$$\widehat{p}_{\varepsilon,\lambda}(\mu_{\theta,\delta,c}) = \begin{cases} \dfrac{2}{n}, & \text{если} \quad \lambda \in (\mathrm{E}_{n,\theta,\varepsilon,c} \cap \overline{\mathrm{E}}_{n,\theta,\varepsilon,c}), \\ \dfrac{1}{n}, & \text{если} \quad \lambda \in (\mathrm{E}_{n,\theta,\varepsilon,c} \cup \overline{\mathrm{E}}_{n,\theta,\varepsilon,c}) \backslash (\mathrm{E}_{n,\theta,\varepsilon,c} \cap \overline{\mathrm{E}}_{n,\theta,\varepsilon,c}), \\ 0, & \text{если} \quad \lambda \notin \mathrm{E}_{n,\theta,\varepsilon,c} \cup \overline{\mathrm{E}}_{n,\theta,\varepsilon,c}. \end{cases} \tag{12}$$

Очевидно, что

$$\widehat{\mathbf{p}}(\mu_{\theta,0,c}) = \widehat{\mathbf{p}}(\mu_{\theta,\delta,c}) \quad \text{для каждого} \quad \delta \in Z_n.$$

Кроме того, так как

$$\widehat{p}_{\varepsilon,\lambda}(\mu_{\theta,\delta,c}) = \widehat{p}_{\varepsilon',\lambda'}(\mu_{\theta,0,0}) \quad \text{при} \quad \varepsilon' = (\varepsilon+c)_{(n)}, \;\; \lambda' = (\lambda+c)_{(n)},$$

то матрицы $\widehat{\mathbf{p}}(\mu_{\theta,\delta,c})$, $\widehat{\mathbf{p}}(\mu_{\theta,0,0})$ различаются перестановками строк и столбцов (циклическим их сдвигом на одинаковое число c). Поэтому достаточно описывать свойства матрицы $\widehat{\mathbf{p}}(\mu_{\theta,0,0})$.

Покажем, что для каждого $i \in \{1, \ldots, 2^{m-1}-1\}$ у матрицы $\widehat{\mathbf{p}}(\mu_{\theta,\delta,0})$ строки (столбцы) с номерами i и $2^m - i$ равны.

Утверждение 5. *Пусть* 2^m+1 *— простое число,* $m \geqslant 1$, $n = 2^m$. *Тогда для всех* $\varepsilon, \lambda \in Z_n^\times$ *справедливы равенства*

$$\widehat{p}_{\varepsilon,\lambda}(\mu_{\theta,\delta,0}) = \widehat{p}_{\varepsilon,2^m-\lambda}(\mu_{\theta,\delta,0}), \quad \widehat{p}_{\varepsilon,\lambda}(\mu_{\theta,\delta,0}) = \widehat{p}_{2^m-\varepsilon,\lambda}(\mu_{\theta,\delta,0}).$$

Кроме того,

$$\widehat{p}_{2^{m-1},\lambda}(\mu_{\theta,\delta,0}) = \begin{cases} 2, & \textit{если} \quad \lambda \equiv 1 \,(\mathrm{mod}\ 2), \\ 0, & \textit{если} \quad \lambda \equiv 0 \,(\mathrm{mod}\ 2). \end{cases} \tag{13}$$

Доказательство. Так как θ — примитивный элемент поля $GF(n+1)$, то

$$\theta^{2^{m-1}} \equiv -1 \,(\mathrm{mod}\ 2^m+1), \tag{14}$$

$$\theta^{2^m} \equiv 1 \,(\mathrm{mod}\ 2^m+1). \tag{15}$$

Зафиксируем произвольные $\varepsilon, \lambda \in Z_n^{\times}$, $\alpha \in Z_n$. Из сравнения (14) следует, что

$$\theta^{\varepsilon+2^{m-1}+\alpha} \equiv -\theta^{\varepsilon+\alpha} (\mathrm{mod}\ 2^m+1), \quad \theta^{2^{m-1}+\alpha} \equiv -\theta^{\alpha} (\mathrm{mod}\ 2^m+1). \tag{16}$$

Тогда из сравнений (16) вытекает, что

$$\begin{aligned}&(\mu_{\theta,\delta,0}(\alpha+2^{m-1}+\varepsilon) - \mu_{\theta,\delta,0}(\alpha+2^{m-1}))_{(n)} = \\ &= 2^m - (\mu_{\theta,\delta,0}(\alpha+\varepsilon) - \mu_{\theta,\delta,0}(\alpha))_{(n)}.\end{aligned}$$

Значит,

$$\widehat{p}_{\varepsilon,\lambda}(\mu_{\theta,\delta,c}) = \widehat{p}_{\varepsilon,2^m-\lambda}(\mu_{\theta,0,c}).$$

Из сравнения (15) имеем

$$\theta^{\varepsilon+\alpha+2^m-\varepsilon} \equiv \theta^{\alpha} (\mathrm{mod}\ 2^m+1).$$

Значит,

$$\begin{aligned}&\big(\mu_{\theta,\delta,0}(\alpha+\varepsilon+2^m-\varepsilon) - \mu_{\theta,\delta,0}(\alpha+\varepsilon)\big)_{(n)} = \\ &= 2^m - \big(\mu_{\theta,\delta,0}(\alpha+\varepsilon) - \mu_{\theta,\delta,0}(\alpha)\big)_{(n)}.\end{aligned}$$

Таким образом, $\widehat{p}_{\varepsilon,\lambda}(\mu_{\theta,\delta,0}) = \widehat{p}_{2^m-\varepsilon,\lambda}(\mu_{\theta,\delta,0})$.

Используя сравнение $\theta^{\alpha+2^{m-1}} \equiv -\theta^{\alpha} (\mathrm{mod}\ 2^m+1)$, получаем, что

$$\big(\mu_{\theta,\delta,0}(\alpha+2^{m-1}) - \mu_{\theta,\delta,0}(\alpha)\big) \equiv -2(\theta^{\alpha})_{(n+1)} + 1 \,(\mathrm{mod}\ n). \tag{17}$$

Из сравнения (17) следует равенство (13). □

Покажем, что подстановка $\mu_{\theta,\delta,0}$ является $+_{\mathbf{W}}$-марковской для некоторого разбиения $\mathbf{W}$.

Утверждение 6. *Пусть* $m \geqslant 1$ *и матрица* $\widehat{\mathbf{p}}(b)$ *подстановки* $b \in S(\mathbb{Z}_{2^m})$ *такова, что справедливо одно из условий*:

1) $\widehat{p}_{i,j}(b) = \widehat{p}_{2^m-i,2^m-j}(b)$ *для каждых* $i, j \in Z_{2^m}^{\times}$,

2) $\widehat{p}_{i,j}(b) = \widehat{p}_{2^m-i,j}(b)$ *для каждых* $i, j \in Z_{2^m}^{\times}$.

Тогда для разбиения $\mathbf{W} = \{W_0, W_1, \ldots, W_{2^{m-1}}\}$, *где*

$$W_i = \begin{cases} \{i, 2^m - i\}, & \text{если} \quad i \in \{1, \ldots, 2^{m-1} - 1\}, \\ \{2^{m-1}\}, & \text{если} \quad i = 2^{m-1}, \\ 0, & \text{если} \quad i = 0, \end{cases} \tag{18}$$

подстановка b *является* $+_{\mathbf{W}}$*-марковской.*

Доказательство. Зафиксируем произвольные числа $i, j \in \{1, \ldots, 2^{m-1}\}$. Если выполнены условия п. 1 утверждения 6, то

$$\widehat{p}_{i,W_j}(b) = \widehat{p}_{i,j}(b) + \widehat{p}_{i,2^m-j}(b) = \\ = \widehat{p}_{2^m-i,2^m-j}(b) + \widehat{p}_{2^m-i,j}(b) = \widehat{p}_{2^m-i,W_j}(b).$$

Если же выполнены условия п. 2 утверждения 6, то

$$\widehat{p}_{i,W_j}(b) = \widehat{p}_{i,j}(b) + \widehat{p}_{i,2^m-j}(b) = \\ = \widehat{p}_{2^m-i,j}(b) + \widehat{p}_{2^m-i,2^m-j}(b) = \widehat{p}_{2^m-i,W_j}(b). \qquad \square$$

Из утверждения 5 следует, что для каждой пары $(\varepsilon, \lambda) \in (Z_n^{\times})^2$ справедливо равенство

$$\widehat{p}_{\varepsilon,\lambda}(\mu_{\theta,\delta,0}) = \widehat{p}_{\varepsilon,2^m-\lambda}(\mu_{\theta,\delta,0}) = \\ = \widehat{p}_{2^m-\varepsilon,\lambda}(\mu_{\theta,\delta,0}) = \widehat{p}_{2^m-\varepsilon,2^m-\lambda}(\mu_{\theta,\delta,0}). \tag{19}$$

Тогда из утверждений 3, 6 вытекает $+_{\mathbf{W}}$-марковость подстановки $\mu_{\theta,\delta,0}$ для разбиения $\mathbf{W}$, у которого блоки задаются равенством (18). Кроме того, для каждого $j \in \{1, \ldots, 2^{m-1}\}$ из равенства (13) получаем, что

$$\widehat{p}_{2^{m-1},W_j}(\mu_{\theta,\delta,0}) = \widehat{p}_{2^{m-1},j}(\mu_{\theta,\delta,0}) + \widehat{p}_{2^{m-1},2^m-j}(\mu_{\theta,\delta,0}) = \\ = 2\,\widehat{p}_{2^{m-1},j}(\mu_{\theta,\delta,0}) = \begin{cases} 4, & \text{если} \quad j \equiv 1 \pmod 2, \\ 0, & \text{если} \quad j \equiv 0 \pmod 2. \end{cases}$$

Пример 1. Пусть $n = 16,\ \theta = 5,\ c = 0,\ \delta \in Z_{16}$ и

$$\mathbf{W} = \{\{0\}, \{1, 15\}, \{2, 14\}, \ldots, \{7, 9\}, \{8\}\}.$$

Из утверждений 3, 5 следует, что $\mu_{5,\delta,0}$ является $+_{\mathbf{W}}$-марковской подстановкой.

В [16] предложено множество экспоненциальных подстановок, включающее в себя класс подстановок $\mu'_\theta : \mathbb{Z}_{2^m} \to GF(2^m)$, заданных условием

$$\mu'_\theta : \alpha \mapsto \begin{cases} 0, & \text{если} \quad \alpha = 0, \\ \theta^\alpha, & \text{если} \quad \alpha \neq 0, \end{cases}$$

где θ — примитивный элемент поля $GF(2^m)$. Пусть $f(x)$ — минимальный многочлен степени m, $GF(2^m) = GF(2)[x]/f(x)$, ϑ — корень многочлена $f(x)$ в поле $GF(2^m)$, $\psi_m : GF(2^m) \to \mathbb{Z}_{2^m}$ — взаимно однозначное отображение, заданное условием

$$\psi_m : \vartheta^{m-1}\alpha_{m-1} \oplus \vartheta^{m-2}\alpha_{m-2} \oplus \ldots \oplus \vartheta\alpha_1 \oplus \alpha_0 \mapsto$$
$$\mapsto 2^{m-1}\alpha_{m-1} + 2^{m-2}\alpha_{m-2} + \ldots + \alpha_0.$$

Утверждение 7. *Справедливо равенство*

$$\widehat{p}_{\varepsilon,\lambda}(\mu'_\theta) = \widehat{p}_{2^m-\varepsilon,\lambda}(\mu'_\theta) \quad \textit{для всех} \quad \varepsilon, \lambda \in Z^\times_{2^m}.$$

Доказательство. Для каждой пары $(\varepsilon, \alpha) \in Z^\times_{2^m} \times Z_{2^m}$ справедливы равенства

$$\mu'_\theta(\alpha + \varepsilon + 2^m - \varepsilon) = \begin{cases} 0, & \text{если} \quad \alpha = 0, \\ \theta^\alpha, & \text{если} \quad \alpha \neq 0, \end{cases}$$

$$\mu'_\theta(\alpha + \varepsilon) = \begin{cases} 0, & \text{если} \quad \alpha + \varepsilon \equiv 0 \,(\mathrm{mod}\ 2^m), \\ \theta^{\alpha+\varepsilon}, & \text{если} \quad \alpha + \varepsilon \not\equiv 0 \,(\mathrm{mod}\ 2^m), \end{cases}$$

из которых следует, что

$$\psi_m(\mu'_\theta(\alpha + \varepsilon + 2^m - \varepsilon)) - \psi_m(\mu'_\theta(\alpha + \varepsilon)) \equiv$$
$$\equiv \psi_m(\mu'_\theta(\alpha + \varepsilon)) - \psi_m(\mu'_\theta(\alpha)) \,(\mathrm{mod}\ 2^m). \qquad \square$$

Из утверждений 6, 7 вытекает $+_{\mathbf{W}}$-марковость подстановки μ'_θ для разбиения $\mathbf{W}$, у которого блоки задаются равенством (18).

Пример 2. Пусть $n = 16$, $m = 4$, $f(x) = x^4 \oplus x \oplus 1$ — минимальный многочлен, $GF(4) = GF(2)[x]/f(x)$. Из утверждений 3, 7 следует, что подстановка μ'_θ является $+_{\mathbf{W}}$-марковской для разбиения

$$\mathbf{W} = \{\{0\}, \{1, 15\}, \{2, 14\}, \ldots, \{7, 9\}, \{8\}\}.$$

5. $+_{\mathbf{W}}$-марковость логарифмических подстановок

Рассмотрим еще один класс $+_{\mathbf{W}}$-марковских подстановок, называемых логарифмическими, также основанных на операциях экспоненцирования и логарифмирования в кольце $\mathbb{Z}_n$ и поле $GF(n+1)$ (для простого числа $n+1$). Логарифмические подстановки были предложены первым автором данной работы и М. Масленниковым. Они применяются в семействе функций хеширования MCSSHA, причем первая функция хеширования этого семейства MCSSHA-1 являлась кандидатом для участия в конкурсе SHA-3. Перемешивающие свойства логарифмических подстановок рассматривались, например, в [17].

О п р е д е л е н и е 10. Пусть $n \in \mathbb{N}$, $n+1$ — простое число, θ — примитивный элемент в поле $GF(n+1)$, $\delta \in GF(n+1)$, $c \in \mathbb{Z}_n$, подстановка $\pi_{\theta,\delta,c} \in S(\mathbb{Z}_n)$ задана условием

$$\pi_{\theta,\delta,c} : x \mapsto$$

$$\mapsto \begin{cases} \log \mathrm{g}_\theta((\theta^{x+c} + \delta)_{(n+1)}), & \text{если} \quad \theta^{x+c} + \delta \not\equiv 0 \,(\mathrm{mod}\ n+1), \\ \log \mathrm{g}_\theta(\delta), & \text{если} \quad \theta^{x+c} + \delta \equiv 0 \,(\mathrm{mod}\ n+1). \end{cases}$$

Элемент $\alpha \in \mathbb{Z}_n$ называется *выколотым* для подстановки $\pi_{\theta,\delta,c}$, если

$$\theta^{\alpha+c} + \delta \equiv 0 \,(\mathrm{mod}\ n+1),$$

а сама подстановка $\pi_{\theta,\delta,c}$ — *логарифмической*.

Покажем, что подстановка $\pi_{\theta,\delta,c}$ является $+_{\mathbf{W}}$-марковской для некоторых разбиений $\mathbf{W}$.

Пусть $\gamma_{\theta,\delta,c}$ — выколотый элемент подстановки $\pi_{\theta,\delta,c}$. Нетрудно убедиться, что существует элемент $\varepsilon_{\theta,\delta,c} \in \mathbb{Z}_n^\times$, для которого

$$(\gamma_{\theta,\delta,c} + \varepsilon_{\theta,\delta,c})^{\pi_{\theta,\delta,c}} \equiv \varepsilon_{\theta,\delta,c} + (\gamma_{\theta,\delta,c})^{\pi_{\theta,\delta,c}} (\mathrm{mod}\, n),$$

$$(\gamma_{\theta,\delta,c})^{\pi_{\theta,\delta,c}} \equiv -\varepsilon_{\theta,\delta,c} + (\gamma_{\theta,\delta,c} - \varepsilon_{\theta,\delta,c})^{\pi_{\theta,\delta,c}} (\mathrm{mod}\, n).$$

Лемма 1. *Пусть* $n+1$ *— простое число. Тогда логарифмическая подстановка* $\pi_{\theta,\delta,c}$ *обладает следующими свойствами*:

1) $\widehat{p}_{\lambda,\lambda}(\pi_{\theta,\delta,c}) = 0$ *для каждого* $\lambda \in \mathbb{Z}_n^\times \setminus \{\varepsilon_{\theta,\delta,c}, n - \varepsilon_{\theta,\delta,c}\}$,

2) $\widehat{p}_{\varepsilon_{\theta,\delta,c},\varepsilon_{\theta,\delta,c}}(\pi_{\theta,\delta,c}) = \widehat{p}_{n-\varepsilon_{\theta,\delta,c},n-\varepsilon_{\theta,\delta,c}}(\pi_{\theta,\delta,c}) = 1$,

3) $\widehat{p}_{\varepsilon_{\theta,\delta,c},n/2}(\pi_{\theta,\delta,c}) = \widehat{p}_{n-\varepsilon_{\theta,\delta,c},n/2}(\pi_{\theta,\delta,c}) = 2$,

4) $(\alpha+\lambda)^{\pi_{\theta,\delta,c}} - \alpha^{\pi_{\theta,\delta,c}} \not\equiv (\alpha'+\lambda)^{\pi_{\theta,\delta,c}} - \alpha'^{\pi_{\theta,\delta,c}}$ *для каждых таких* $\alpha, \alpha' \in \mathbb{Z}_{2^n} \setminus \{\gamma_{\theta,\delta,c}\}$, $\lambda \in \mathbb{Z}_n^\times$, *что* $\gamma_{\theta,\delta,c} \notin \{\alpha+\lambda, \alpha'+\lambda\}$,

5) *для каждого* $\lambda \in \mathbb{Z}_n^\times$ *справедливо равенство*

$$\left\{(\alpha+\lambda)^{\pi_{\theta,\delta,c}} - \alpha^{\pi_{\theta,\delta,c}} \,\middle|\, \alpha \in \mathbb{Z}_n \setminus \{\gamma_{\theta,\delta,c}, \gamma_{\theta,\delta,c} - \lambda\}\right\} = \mathbb{Z}_n^\times \setminus \{\lambda\},$$

6) *для каждого* $\lambda \in \mathbb{Z}_n^\times \setminus \{\varepsilon_{\theta,\delta,c},\ n - \varepsilon_{\theta,\delta,c}\}$ *существуют такие элементы* $\omega_\lambda, \omega'_\lambda \in \mathbb{Z}_n^\times \setminus \{\varepsilon_{\theta,\delta,c},\ n - \varepsilon_{\theta,\delta,c},\ \lambda\}$, $\omega \neq \omega'$, *что справедливы соотношения*

$$(\gamma_{\theta,\delta,c} + \lambda)^{\pi_{\theta,\delta,c}} - (\gamma_{\theta,\delta,c})^{\pi_{\theta,\delta,c}} \equiv \omega_\lambda \pmod n,$$
$$(\gamma_{\theta,\delta,c})^{\pi_{\theta,\delta,c}} - (\gamma_{\theta,\delta,c} - \lambda)^{\pi_{\theta,\delta,c}} \equiv \omega'_\lambda \pmod n,$$

$$\widehat{p}_{\lambda,\omega_\lambda}(\pi_{\theta,\delta,c}) = \widehat{p}_{\lambda,\omega'_\lambda}(\pi_{\theta,\delta,c}) = \widehat{p}_{n-\lambda,n-\omega_\lambda}(\pi_{\theta,\delta,c}) =$$
$$= \widehat{p}_{n-\lambda,n-\omega'_\lambda}(\pi_{\theta,\delta,c}) = \frac{2}{n},$$
$$\widehat{p}_{\lambda,\tau}(\pi_{\theta,\delta,c}) = \frac{1}{n} \quad \textit{для каждого} \quad \tau \in \mathbb{Z}_n^\times \setminus \{\lambda, \omega_\lambda, \omega'_\lambda\}.$$

Доказательство известно и имеет технический характер. □

Так как

$$\begin{aligned} \omega_\lambda &\equiv (\gamma_{\theta,\delta,c} + \lambda)^{\pi_{\theta,\delta,c}} - (\gamma_{\theta,\delta,c})^{\pi_{\theta,\delta,c}} \equiv \\ &\equiv \log_\theta \log\left(\delta\left((1-\theta^\lambda)_{(n+1)}\right)\right) - \log_\theta(\delta) \equiv \log_\theta\left((1-\theta^\lambda)_{(n+1)}\right) \pmod n, \end{aligned} \tag{20}$$

$$\begin{aligned} \omega'_\lambda &\equiv (\gamma_{\theta,\delta,c})^{\pi_{\theta,\delta,c}} - (\gamma_{\theta,\delta,c} - \lambda)^{\pi_{\theta,\delta,c}} \equiv \\ &\equiv \log_\theta(\delta) - \log_\theta\left(\delta\left((1-\theta^{-\lambda})_{(n+1)}\right)\right) \equiv \\ &\equiv -\log_\theta\left((1-\theta^{-\lambda})_{(n+1)}\right) \equiv \lambda - \log_\theta\left((\theta^\lambda - 1)_{(n+1)}\right) \pmod n, \end{aligned} \tag{21}$$

то

$$(\gamma_{\theta,\delta,c}+\omega_\lambda)^{\pi_{\theta,\delta,c}}-(\gamma_{\theta,\delta,c})^{\pi_{\theta,\delta,c}}\equiv$$

$$\equiv\log_\theta\big(-\theta^{\log_\theta((1-\theta^\lambda)_{(n+1)})}\delta+\delta\big)-\log_\theta(\delta)\equiv\lambda\,(\mathrm{mod}\,n),$$

$$(\gamma_{\theta,\delta,c})^{\pi_{\theta,\delta,c}}-(\gamma_{\theta,\delta,c}-\omega'_\lambda)^{\pi_{\theta,\delta,c}}\equiv$$

$$\equiv\log_\theta(\delta)-\log_\theta\big(-\theta^{\log_\theta((1-\theta^{-\lambda})_{(n+1)})}\delta+\delta\big)\equiv\lambda\,(\mathrm{mod}\,n).$$

Отсюда и из леммы 1 следует, что $\widehat{p}_{\lambda,\lambda'}(\pi_{\theta,\delta,c})=\widehat{p}_{\lambda',\lambda}(\pi_{\theta,\delta,c})$ для всех $(\lambda,\lambda')\in(\mathbb{Z}_n^\times)^2$.

Так как матрица $\widehat{\mathbf{p}}(\pi_{\theta,\delta,c})$ симметрична относительно главной диагонали, то логарифмической подстановке $\pi_{\theta,\delta,c}$ соответствует граф $\Gamma_{\theta,\delta,c}$ с множеством вершин $\mathbb{Z}_n^\times$ и множеством ребер

$$\Lambda_{\theta,\delta,c}=\big\{(\lambda,\tau)\in(\mathbb{Z}_n^\times)^2\,\big|\,\widehat{p}_{\lambda,\tau}(\pi_{\theta,\delta,c})=2/n\big\}.$$

Опишем компоненты связности графа $\Gamma_{\theta,\delta,c}$, которые далее понадобятся для указания разбиений $\mathbf{W}$, относительно которых подстановка $\pi_{\theta,\delta,c}$ является $+_{\mathbf{W}}$-марковской.

Пусть $\mathrm{E}_{\theta,\delta,c}(\lambda)$ — множество вершин и $\Lambda_{\theta,\delta,c}(\lambda)$ — множество ребер компоненты связности графа $\Gamma_{\theta,\delta,c}$, содержащей вершину $\lambda\in\mathbb{Z}_n^\times$, и $\Gamma_{\theta,\delta,c}(\lambda)=(\mathrm{E}_{\theta,\delta,c}(\lambda),\Lambda_{\theta,\delta,c}(\lambda))$ — соответствующая компонента связности.

Лемма 2. 1. *Если* $\lambda\in\{\varepsilon_{\theta,\delta,c},\,n-\varepsilon_{\theta,\delta,c},\,n/2\}$, *то*

$$\mathrm{E}_{\theta,\delta,c}(\varepsilon_{\theta,\delta,c})=\{\varepsilon_{\theta,\delta,c},\;n-\varepsilon_{\theta,\delta,c},\;n/2\},$$
$$\Lambda_{\theta,\delta,c}(\varepsilon_{\theta,\delta,c})=\{(\varepsilon_{\theta,\delta,c},\,n/2),\;(n-\varepsilon_{\theta,\delta,c},\,n/2)\}.$$

2. *Если* $\lambda\in\mathbb{Z}_n^\times\setminus\{\varepsilon_{\theta,\delta,c},\,n-\varepsilon_{\theta,\delta,c},\,n/2\}$, *то*

$$\mathrm{E}_{\theta,\delta,c}(\lambda)=\big\{\lambda,n-\lambda,\log_\theta\big((1-\theta^\lambda)_{(n+1)}\big),\;n-\log_\theta\big((1-\theta^\lambda)_{(n+1)}\big),$$
$$\log_\theta((1-\theta^{-\lambda})_{(n+1)}),n-\log_\theta\big((1-\theta^{-\lambda})_{(n+1)}\big)\big\},$$

$$\Lambda_{\theta,\delta,c}(\lambda)=\big\{\big(\log_\theta\big((1-\theta^\lambda)_{(n+1)}\big),\;\log_\theta\big((1-\theta^{-\lambda})_{(n+1)}\big)\big),$$
$$\big(\log_\theta\big((1-\theta^{-\lambda})_{(n+1)}\big),-\lambda\big),\;\big(-\lambda,-\log_\theta\big((1-\theta^\lambda)_{(n+1)}\big)\big),$$
$$\big(-\log_\theta\big((1-\theta^\lambda)_{(n+1)}\big),-\log_\theta\big((1-\theta^{-\lambda})_{(n+1)}\big)\big),$$
$$\big(\lambda,\,\log_\theta\big((1-\theta^\lambda)_{(n+1)}\big)\big),\;\big(-\log_\theta\big((1-\theta^{-\lambda})_{(n+1)}\big),\lambda\big)\big\}.$$

Доказательство следует из сравнений (20), (21) и леммы 1. □

Заметим, что число нулевых элементов матрицы вероятностей переходов разностей подстановки $\mu_{\theta,\delta,c}$ больше, чем соответствующее число для логарифмической подстановки $\pi_{\theta,\delta,c}$.

Таким образом, если $n = 4+6q$ для некоторого $q \in \mathbb{N}_0$, то граф $\Gamma_{\theta,\delta,c}$ состоит из $(q+1)$ компонент связности, из которых изоморфны все q компонент, отличные от $\Gamma_{\theta,\delta,c}(\varepsilon_{\theta,\delta,c})$. Пусть $\Gamma_{\theta,\delta,c}(\lambda_1), \ldots, \Gamma_{\theta,\delta,c}(\lambda_q)$ — попарно различные изоморфные компоненты связности графа $\Gamma_{\theta,\delta,c}$, где $\lambda_1, \ldots, \lambda_q \in \in \mathbb{Z}_n^{\times} \setminus \{\varepsilon_{\theta,\delta,c}, n-\varepsilon_{\theta,\delta,c}, n/2\}$.

Покажем теперь существование таких разбиений множеств вершин компонент связностей графа $\Gamma_{\theta,\delta,c}$, задающих соответствующие разбиения $\mathbf{W}$ множества $\{0,\ldots,n-1\}$, что подстановка $\pi_{\theta,\delta,c}$ является $+_{\mathbf{W}}$-марковской.

Для каждого $\lambda_0 \in \{\varepsilon_{\theta,\delta,c}, n-\varepsilon_{\theta,\delta,c}, n/2\}$ рассмотрим два разбиения

$$W^{(0,0)} = \{W_0^{(0,0)}, W_1^{(0,0)}\}, \quad W^{(0,1)} = \big\{\{\gamma\} \,\big|\, \gamma \in \mathrm{E}_{\theta,\delta,c}(\lambda_0)\big\}$$

множества вершин $\mathrm{E}_{\theta,\delta,c}(\lambda_0)$, где

$$W_0^{(0,0)} = \{n/2\}, \quad W_1^{(0,0)} = \{\varepsilon_{\theta,\delta,c},\ n-\varepsilon_{\theta,\delta,c}\}.$$

Для $i \in \{0,1\}$ положим

$$r^{(0,i)} = \big|W^{(0,i)}\big| = \begin{cases} 2, & \text{если} \quad i=0, \\ 3, & \text{если} \quad i=1. \end{cases}$$

Разбиения $W^{(0,0)}$, $W^{(0,1)}$ множества $\mathrm{E}_{\theta,\delta,c}(\lambda_j)$ определены исходя из того, что для каждых $i \in \{0,1\}$, $\gamma \in W_b^{(0,i)}$, $b,t \in \{0,\ldots,r^{(0,i)}-1\}$ справедливо равенство $\sum\limits_{\gamma' \in W_t^{(0,i)}} \widehat{p}_{\gamma,\gamma'}(\pi_{\theta,\delta,c}) = a_{b,t}^{(0,i)}$, где

$$a_{b,t}^{(0,i)} = \begin{cases} 0, & \text{если} \quad i \in \{0,1\},\ b=t=0, \\ 1, & \text{если} \quad i \in \{0,1\},\ b \neq 0,\ t \neq 0, \\ 2, & \text{если} \quad i \in \{0,1\},\ b \neq t,\ b \cdot t = 0. \end{cases} \tag{22}$$

Для $\lambda_j \in \mathbb{Z}_n^{\times} \setminus \{\varepsilon_{\theta,\delta,c}, n-\varepsilon_{\theta,\delta,c}, n/2\}$, $j \in \{1,\ldots,q\}$ обозначим

$$\lambda_j^{(0)} = \lambda_j, \quad \lambda_j^{(1)} = \log_\theta\big((1-\theta^{\lambda_j})_{(n+1)}\big),$$

$$\lambda_j^{(2)} = \log_\theta\big((1-\theta^{-\lambda_j})_{(n+1)}\big), \quad \lambda_j^{(3)} = -\lambda_j,$$

$$\lambda_j^{(4)} = -\log_\theta\big((1-\theta^{\lambda_j})_{(n+1)}\big), \quad \lambda_j^{(5)} = -\log_\theta\big((1-\theta^{-\lambda_j})_{(n+1)}\big).$$

Заметим, что в этих обозначениях

$$\Lambda_{\theta,\delta,c}(\lambda_j) = \big\{(\lambda_j^{(t)}, \lambda_j^{(t+1)}) \big| t = 0, \ldots, 4\big\} \cup \big\{(\lambda_j^{(5)}, \lambda_j^{(0)})\big\}.$$

Рассмотрим следующие разбиения множества $\mathrm{E}_{\theta,\delta,c}(\lambda_j)$:

$$W^{(j,0)} = \mathrm{E}_{\theta,\delta,c}(\lambda_j), \quad W^{(j,1)} = \{W_t^{(j,1)} \,|\, t = 0, 1, 2\},$$

$$W^{(j,2)} = \{W_t^{(j,2)} \,|\, t = 0, 1, 2\}, \quad W^{(j,3)} = \{W_0^{(j,3)}, W_1^{(j,3)}\},$$

$$W^{(j,4)} = \{W_t^{(j,4)} \,|\, t = 0, \ldots, 5\},$$

где

$$W_0^{(j,1)} = \{\lambda_j^{(0)}, \lambda_j^{(1)}\}, \;\; W_1^{(j,1)} = \{\lambda_j^{(2)}, \lambda_j^{(5)}\}, \;\; W_2^{(j,1)} = \{\lambda_j^{(3)}, \lambda_j^{(4)}\},$$

$$W_t^{(j,1)} = \{\lambda_j^{(t)}, \lambda_j^{(3+t)}\} \quad \text{для} \quad t = 0, 1, 2,$$

$$W_t^{(j,3)} = \{\lambda_j^{(t)}, \lambda_j^{(t+2)}, \lambda_j^{(t+4)}\} \quad \text{для} \quad t = 0, 1,$$

$$W_t^{(j,4)} = \{\lambda_j^{(t)}\} \quad \text{для} \quad t = 0, \ldots, 5.$$

Отметим, что из определения разбиений $W^{(j,0)}, \ldots, W^{(j,4)}$ следуют равенства

$$|W^{(1,i)}| = \cdots = |W^{(q,i)}| \quad \text{для всех} \quad i \in \{0, \ldots, 4\}.$$

Поэтому для $i \in \{0, \ldots, 4\}$ положим

$$r^{(j,i)} = |W^{(j,i)}| = \begin{cases} 1, & \text{если} \quad i = 0, \; j \in \{1, \ldots, q\}, \\ 3, & \text{если} \quad i \in \{1, 2\}, \; j \in \{1, \ldots, q\}, \\ 2, & \text{если} \quad i = 3, \; j \in \{1, \ldots, q\}, \\ 6, & \text{если} \quad i = 4, \; j \in \{1, \ldots, q\}. \end{cases} \tag{23}$$

Разбиения $W^{(j,0)},\dots,W^{(j,4)}$ множества $\mathrm{E}_{\theta,\delta,c}(\lambda_j)$ характеризуются тем, что для каждых $i\in\{1,\dots,4\}$, $\gamma\in W_b^{(j,i)}$, $b,\ t\in\{0,\dots,r^{(j,i)}-1\}$ справедливо равенство $\sum\limits_{\gamma'\in W_t^{(j,i)}}\widehat{p}_{\gamma,\gamma'}(\pi_{\theta,\delta,c})=a_{b,t}^{(j,i)}$, где

$$a_{b,t}^{(j,i)}=\begin{cases}\dfrac{4}{n}, & \text{если} \quad i=0,\\ \dfrac{2}{n}, & \text{если} \quad i=1,\ |b-t|\leqslant 1,\\ 0, & \text{если} \quad i=1,\ |b-t|=2,\\ \dfrac{2}{n}, & \text{если} \quad i=2,\ b\neq t,\\ 0, & \text{если} \quad i\in\{2,3\},\ b=t,\\ \dfrac{4}{n}, & \text{если} \quad i=3,\ b\neq t,\\ \dfrac{2}{n}, & \text{если} \quad i=4,\ |b-t|=1,\\ 0, & \text{если} \quad i=4,\ |b-t|\neq 1.\end{cases} \tag{24}$$

Из равенств (22) и (24) следует, что для разбиений $W^{(0,0)}$, $W^{(0,1)}$ и $W^{(j,0)},\dots,W^{(j,4)}$ при $j\in\{1,\dots,q\}$ выполняется утверждение 3.

Для $j\in\{0,\dots,q\}$ положим

$$v^{(j)}=\begin{cases}2, & \text{если} \quad j=0,\\ 5, & \text{если} \quad j\in\{1,\dots,q\}.\end{cases}$$

Из леммы 2 вытекает, что для каждых $j_1,j_2\in\{0,1,\dots,q\}$ при $j_1\neq j_2$, $i_1\in\{0,1,\dots,v^{(j_1)}\}$, $i_2\in\{0,1,\dots,v^{(j_2)}\}$, $t_1\in\{0,1,\dots,r^{(j_1,i_1)}-1\}$, $t_2\in\{0,1,\dots,r^{(j_2,i_2)}-1\}$ и $\gamma\in W_{t_1}^{(j_1,i_1)}$ справедливо равенство

$$\sum_{\gamma'\in W_{t_2}^{(j_2,i_2)}}\widehat{p}_{\gamma,\gamma'}(\pi_{\theta,\delta,c})=\frac{|W_{t_2}^{(j_2,i_2)}|}{n}. \tag{25}$$

Из равенства (24) следует, что разбиения $W^{(0,0)}$, $W^{(0,1)}$ и $W^{(j,0)},\dots,W^{(j,4)}$ при $j\in\{1,\dots,q\}$ удовлетворяют условиям утверждения 3.

Утверждение 8. *Пусть*:

1) $n = 4 + 6q$, *где* $q \in \mathbb{N}_0$, $n+1$ — *простое число,* θ — *примитивный элемент поля* $GF(n+1)$, $\delta \in GF(n+1)$, $c \in \mathbb{Z}_n$,

2) $\Gamma_{\theta,\delta,c}(\lambda_1), \ldots, \Gamma_{\theta,\delta,c}(\lambda_q)$ — *попарно различные изоморфные компоненты связности графа* $\Gamma_{\theta,\delta,c}$, *где*

$$\lambda_1, \ldots, \lambda_q \in \mathbb{Z}_n^{\times} \setminus \{\varepsilon_{\theta,\delta,c}, n - \varepsilon_{\theta,\delta,c}, n/2\},$$

3) $\lambda_0 \in \{\varepsilon_{\theta,\delta,c}, n - \varepsilon_{\theta,\delta,c}, n/2\}$,

4) i_j — *произвольный элемент множества* $\{0, \ldots, v^{(j)} - 1\}$ *для каждого* $j \in \{0, \ldots, q\}$.

Тогда подстановка $\pi_{\theta,\delta,c}$ *является* $+_{\mathbf{W}}$*-марковской для следующих разбиений* $\mathbf{W}$:

А. *Разбиение* $\mathbf{W}$, *блоками которого являются множества*

$$W_0^{(j,i_j)}, \ldots, W_{r^{(j,i_j)}-1}^{(j,i_j)} \quad \text{для всех} \quad j \in \{0, \ldots, q\}.$$

Б. *Разбиение* $\mathbf{W}$, *блоками которого являются множества*

$$W_0^{(0,i_0)}, \ldots, W_{r^{(0,i_0)}-1}^{(0,i_0)},$$

а также множества, полученные произвольным объединением множеств $\mathrm{E}_{\theta,\delta,c}(\lambda_1), \ldots, \mathrm{E}_{\theta,\delta,c}(\lambda_q)$.

Доказательство следует из равенств (22), (24) и (25). □

Логарифмическая подстановка $\pi_{\theta,\delta,c}$ является $\otimes_{\mathbf{W}}^{(J)}$-марковской для

$$\mathbf{W} = \left\{\mathrm{E}_{\theta,\delta,c}(\lambda_i) \mid i \in \{0, \ldots, q\}\right\}, \quad J = \{1, \ldots, q\}.$$

6. $\oplus_{\mathbf{W}}$-марковость APN-подстановок

Рассмотрим теперь связь между $\oplus_{\mathbf{W}}$-марковостью APN-подстановок и их свойствами, которые также являются преобразованиями нелинейного слоя XSL-алгоритмов блочного шифрования на V_n.

О п р е д е л е н и е 11 ([18]). APN-*подстановкой* $b \in S(V_n)$ называется подстановка, удовлетворяющая равенству

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

Из определения 11 следует, что у любой APN-подстановки $b \in S(V_n)$ наибольший элемент каждой строки матрицы вероятностей переходов разностей $\widehat{\mathbf{p}}(b)$ равен 2^{1-n}. Данное значение является наименьшим среди всех подстановок из $S(V_n)$. Поэтому APN-подстановки считаются (см. [18]) оптимальными для использования в качестве подстановок S-боксов для улучшения стойкости алгоритма блочного шифрования относительно разностного метода.

Каждой APN-подстановке поставим в соответствие орграф $\Gamma(b)$ с множеством вершин $V_n^{\times}$ и множеством дуг, определяемый $(2^n-1)\times(2^n-1)$-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

$$q_{i,j}(b) = \begin{cases} 1, & \text{если} \quad \widehat{p}_{i,j}(b) = \dfrac{1}{2^{n-1}}, \\ 0, & \text{если} \quad \widehat{p}_{i,j}(b) = 0. \end{cases}$$

Ясно, что в каждой строке и каждом столбце матрицы $\mathbf{q}(b)$ число единиц равно 2^{n-1}, а число нулей равно $2^{n-1}-1$. Заметим, что матрица $\mathbf{q}(b)$ является симметричной тогда и только тогда, когда $\widehat{\mathbf{p}}(b) = \widehat{\mathbf{p}}(b^{-1})$.

Для APN-подстановки $b \in S(V_n)$ укажем связь между элементами группы автоморфизмов орграфа $\Gamma(b)$ и ее $\oplus_{\mathbf{W}}$-марковостью.

Утверждение 9. *Пусть b — произвольная APN-подстановка на V_n.*

Тогда для каждого элемента

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

подстановка b является $\oplus_{\mathbf{W}^{(g)}}$-марковской для разбиения $\mathbf{W}^{(g)} = \{W_0,\dots,W_r\}$, где $W_0 = \{\vec{0}_n\}$ и $W_j = \{\alpha_1^{(j)},\dots,\alpha_{d_j}^{(j)}\}$ для $j = 1,\dots,r$.

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

$$\frac{1}{2^n}\sum_{\theta' \in W_j} q_{\theta,\theta'}(b) = \sum_{\theta' \in W_j} \widehat{p}_{\theta,\theta'}(b) = \widehat{p}_{\theta,W_j}(b), \tag{26}$$

и $\sum_{\theta' \in W_j} q_{\theta,\theta'}(b)$ — число дуг, исходящих из вершины θ в вершины, принадлежащие множеству W_j. Так как $g \in \mathrm{Aut}(\Gamma(b))$, то для каждого $c \in \{1,\dots,d_i\}$ число дуг, исходящих из вершины θ^{g^c} в вершины, принадлежащие множеству W_j, будет одно и то же и равно некоторому числу $a_{i,j}(b) \in \mathbb{N}_0$. Таким образом, из равенства (26) вытекает, что $\widehat{p}_{\theta,W_j}(b) = a_{i,j}(b)/2^n$ для всех $\theta \in W_i$, $i,j \in \{0,\dots,r\}$. Из утверждения 3 следует $\oplus_{\mathbf{W}^{(g)}}$-марковость подстановки b. □

Для некоторых APN-подстановок b приведем группу автоморфизмов орграфа $\Gamma(b)$ и укажем такие разбиения $\mathbf{W}$ пространства V_n, что:

1) b — $\oplus_{\mathbf{W}}$-марковская подстановка;

2) разбиение $\mathbf{W}$ определяется цикловой структурой элемента группы автоморфизмов $\mathrm{Aut}(\Gamma(b))$, соответствующее задание описано в утверждении 9.

Приведем соответствующие примеры.

1. Пусть

$$m = 3, \quad GF(2^3) = GF(2)[\alpha]/(\alpha^3 \oplus \alpha \oplus 1), \quad \gamma \in GF(2^3)$$

и APN-подстановка $b_1 \in S(GF(2^3))$ задана условием

$$b_1 : x \mapsto \begin{cases} x^{-1} \oplus \gamma, & \text{если} \quad x \neq 0, \\ \gamma, & \text{если} \quad x = 0. \end{cases}$$

Тогда матрица $\mathbf{q}(b_1)$ симметрическая,

$$\mathrm{Aut}(\Gamma(b_1)) =$$

$$= \{e, (4,6)(5,7), (2,4)(3,5), (2,6)(3,7), (2,4,6)(3,5,7), (2,6,4)(3,7,5)\},$$

а матрица вероятностей переходов разностей подстановки b_1 равна

$$\widehat{\mathbf{p}}(b_1) = \frac{1}{2^3} \begin{pmatrix} 2 & 0 & 2 & 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 2 & 2 & 2 & 2 \\ 2 & 0 & 2 & 2 & 0 & 2 & 0 \\ 0 & 2 & 2 & 0 & 0 & 2 & 2 \\ 2 & 2 & 0 & 0 & 2 & 2 & 0 \\ 0 & 2 & 2 & 2 & 2 & 0 & 0 \\ 2 & 2 & 0 & 2 & 0 & 0 & 2 \end{pmatrix}.$$

Подстановка b_1 является $\oplus_{\mathbf{W}}$-марковской только для десяти разбиений $\mathbf{W}^{(1)}, \ldots, \mathbf{W}^{(10)}$:

$$\mathbf{W}^{(1)} = \{\{0\},\{1\},\{6\},\{7\},\{2,4\},\{3,5\}\},$$
$$\mathbf{W}^{(2)} = \{\{0\},\{1\},\{2\},\{3\},\{5,7\},\{4,6\}\},$$
$$\mathbf{W}^{(3)} = \{\{0\},\{1\},\{4\},\{5\},\{3,7\},\{2,6\}\},$$
$$\mathbf{W}^{(4)} = \{\{0\},\{1\},\{2,4,6\},\{3,5,7\}\},$$
$$\mathbf{W}^{(5)} = \{\{0\},\{3\},\{1,4,6\},\{2,5,7\}\},$$
$$\mathbf{W}^{(6)} = \{\{0\},\{2\},\{1,3\},\{4,5,6,7\}\},$$
$$\mathbf{W}^{(7)} = \{\{0\},\{4\},\{1,5\},\{2,3,6,7\}\},$$
$$\mathbf{W}^{(8)} = \{\{0\},\{6\},\{1,7\},\{2,3,4,5\}\},$$
$$\mathbf{W}^{(9)} = \{\{0\},\{1,2,6\},\{3,4,7\},\{5\}\},$$
$$\mathbf{W}^{(10)} = \{\{0\},\{7\},\{1,2,4\},\{3,5,6\}\}.$$

При этом разбиения $\mathbf{W}^{(1)}, \ldots, \mathbf{W}^{(4)}$ соответствуют неединичным элементам группы $\mathrm{Aut}(\Gamma(b_1))$, а разбиения $\mathbf{W}^{(5)}, \ldots, \mathbf{W}^{(10)}$ являются объединениями разбиений $\mathbf{W}^{(1)}, \ldots, \mathbf{W}^{(4)}$. В частности, для каждого $j \in \{1, \ldots, 10\}$ существует неединичный элемент, принадлежащий группе $\mathrm{Aut}(\Gamma(b_1))$ и сохраняющий разбиение $\mathbf{W}^{(j)}$.

Заметим, что при $n = 4$ преобразование обращения на $GF(2^4)$, заданное аналогично подстановке b_1, не является APN-подстановкой.

2. Пусть $m = 3$, $GF(2^3) = GF(2)/(\alpha^3 \oplus \alpha \oplus 1)$ и APN-подстановка $b_2 \in S(GF(2^3))$ задана условием $b_2 : x \mapsto x^5$. Тогда

$$\mathrm{Aut}(\Gamma(b_2)) = \{e, (2,4,6)(3,5,7), (2,6,4)(3,7,5)\},$$

и подстановка b_2 является $\oplus_{\mathbf{W}}$-марковской только для разбиения $\mathbf{W} = \mathbf{W}^{(5)}$, которому соответствуют элементы (2,4,6)(3,5,7), (2,6,4)(3,7,5) группы $\mathrm{Aut}(\Gamma(b_2))$. При этом

$$\widehat{\mathbf{p}}_{\mathbf{W}}(b_2) = \frac{1}{2^3} \begin{pmatrix} 8 & 0 & 0 & 0 \\ 0 & 2 & 0 & 6 \\ 0 & 0 & 4 & 4 \\ 0 & 2 & 4 & 2 \end{pmatrix}.$$

3. Нетрудно убедиться, например, перебором всех таких подстановок с помощью компьютера, что APN-подстановки на пространстве V_3 обладают следующими свойствами:

   А. Число всех APN-подстановок на V_3 равно 10752.

   Б. Матрица вероятностей переходов разностей каждой APN-подстановки на V_3 отличается от матрицы $\widehat{\mathbf{p}}(b_1)$ только перестановкой строк.

   В. Все строки и столбцы матрицы $\mathbf{q}(b_1)$ ортогональны над полем $GF(2)$. Отсюда и из п. Б следует, что все строки и столбцы матрицы $\mathbf{q}(b)$ каждой APN-подстановки b на V_3 ортогональны над полем $GF(2)$. Поэтому матрицу $\mathbf{q}(b)$ можно считать аналогом матрицы Адамара.

Заметим, что наличие $\oplus_{\mathbf{W}}$-марковости у приведенных примеров APN-подстановок обусловлено оптимальностью матриц вероятностей переходов разностей для данных подстановок относительно разностного метода.

Список литературы

[1] Minier M., Gilbert H., “Stochastic cryptanalysis of Crypton”. In: “*FSE 2000*”, Lect. Notes Comput. Sci., **1978**, 2000, 121–133.

[2] Lai X., Massey J. L., Murphy S., “Markov ciphers and differential cryptanalysis”. In: “*EuroCrypt 1991*”, Lect. Notes Comput. Sci., **547**, 1991, 17–38.

[3] Кемени Д., Снелл Д., *Конечные цепи Маркова*, М.: Наука, 1970, 272 с.

[4] Сачков В. Н., “Вероятностные преобразователи и правильные мультиграфы. I”, *Труды по дискретной математике*, **1** (1997), 227–250.

[5] Сачков В. Н., “Цепи Маркова итерационных систем преобразований”, *Труды по дискретной математике*, **6** (2002), 165–183.

[6] Сачков В. Н., “Вероятностные преобразователи и суммы элементарных матриц. II”, *Труды по дискретной математике*, **8** (2005), 240–252.

[7] Максимов Ю. И., “Некоторые результаты для задачи укрупнения состояний цепей Маркова”, *Труды по дискретной математике*, **8** (2005), 148–154.

[8] Vaudenay S., “On the Lai – Massey scheme”. In: “*ASIACRYPT’99*”, Lect. Notes Comput. Sci., **1716**, 1999, 8–19.

[9] Knudsen L. R., “Truncated and higher order differentials”. In: “*FSE’95*”, Lect. Notes Comput. Sci., **1008**, 1995, 196–211.

[10] Matsui M., Tokita T., “Cryptanalysis of a reduced version of the block cipher E2”. In: “*FSE’99*”, Lect. Notes Comput. Sci., 1999, 70–79.

[11] Moriai S., Sugita M., Aoki K., Kanda M., “Security of E2 against truncated differential cryptanalysis”. In: “*SAC’99*”, Lect. Notes Comput. Sci., **1758**, 2000, 106–117.

[12] Reichardt B., Wagner D., “Markov truncated differential cryptanalysis of Skipjack”. In: “*SAC 2002*”, Lect. Notes Comput. Sci., **2595**, 2002, 110—128.

[13] Blondeau C., “Improbable differential from impossible differential: on the validity of the model”. In: “*INDOCRYPT 2013*”, Lect. Notes Comput. Sci., **8250**, 2013, 149–160.

[14] Massey J.L., “SAFER K-64: One year later”. In: “*FSE'94*”, Lect. Notes Comput. Sci., **1008**, 1994, 212–232.

[15] Lai X., *On the design and security of block ciphers*, Zurich, Swiss Federal Inst. Technology, PhD, 1992.

[16] Агиевич С. В., Афоненко А. А., “Экспоненциальные S-блоки”, В сб.: *Математика и безопасность информационных технологий*. МАБИТ 2003, М. : МЦНМО, 2003, 127–130.

[17] Шемякина О. В., “Об оценке характеристик разбиений различных алгебраических структур”, В сб.: Информ. безопасность регионов России ИБРР-2011. Матер. VII СПб. межрегион. конф., СПб. : СПОИСУ, 2011, 137.

[18] Nyberg K., Knudsen L. R., “Provable security against differential cryptanalysis”. In: “*Crypto 1992*”, Lect. Notes Comput. Sci., **740**, 1993, 566–574.