УДК 519.7 DOI 10.17223/2226308X/8/25

$\otimes_{\mathbf{W},\mathrm{ch}}$-МАРКОВОСТЬ И ИМПРИМИТИВНОСТЬ В БЛОЧНЫХ ШИФРСИСТЕМАХ

Б. А. Погорелов, М. А. Пудовкина

Рассмотрена связь между $\otimes_{\mathbf{W},\mathrm{ch}}$-марковостью итеративных алгоритмов блочного шифрования и методом гомоморфизмов. Для алгоритмов блочного шифрования и разбиений $\mathbf{W}$ алфавита текстов X, блоки которых являются смежными классами по некоторой подгруппе абелевой регулярной группы $(X, \otimes)$, доказана эквивалентность между $\otimes_{\mathbf{W},\mathrm{ch}}$-марковостью алгоритма и существованием нетривиального гомоморфизма. Показано, что класс $\otimes_{\mathbf{W},\mathrm{ch}}$-марковских преобразований не ограничивается только упомянутыми разбиениями. Так, для разбиений $\mathbf{W}$, блоки которых не являются смежными классами по подгруппе аддитивной группы $(V_n^+, \oplus)$ векторного пространства V_n, описаны классы аффинных и нелинейных $\oplus_{\mathbf{W},\mathrm{ch}}$-марковских преобразований. Приведены условия на разбиения $\mathbf{W}$ пространства V_n, при которых аффинное преобразование является $\oplus_{\mathbf{W},\mathrm{ch}}$-марковским. Получено, что для каждого разбиения $\mathbf{W}$ пространства V_n множество всех $\oplus_{\mathbf{W},\mathrm{ch}}$-марковских преобразований из AGL_n является группой. Приведены примеры таких групп. Тем самым показано, что для данного класса разбиений $\otimes_{\mathbf{W},\mathrm{ch}}$-марковость является обобщением рассмотренных гомоморфизмов.

Ключевые слова: *импримитивная группа, метод гомоморфизмов, XSL-алгоритмы блочного шифрования, сплетение групп подстановок.*

Пусть $(X, \otimes)$ — произвольная регулярная абелева группа на конечном множестве X с бинарной операцией $\otimes$ и единичным элементом e; $X^\times = X \setminus \{e\}$; $S(X)$ — симметрическая группа на X; $\alpha^g = \alpha g = g(\alpha)$ — образ элемента $\alpha \in X$ при действии на него подстановкой $g \in S(X)$; AGL_n — полная аффинная группа над V_n; G_α — стабилизатор элемента $\alpha \in V_n$; $G \leqslant S(V_n)$; AG — аффинная подгруппы группы AGL_n при $G \leqslant GL_n$ и $G = AG_{\mathbf{0}}$. Пусть также $IG_{\mathbf{W}} = (S_w \wr S_r, \mathbf{W})$ — максимальная группа подстановок на $X = W_0 \cup \ldots \cup W_{r-1}$, сохраняющая разбиение $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$, где $w = |W_0| = \ldots = |W_{r-1}|$. Эта группа называется сплетением группы подстановок S_w группой S_r.

Рассмотрим l-раундовый алгоритм блочного шифрования, у которого раундовая функция $g : X^2 \to X$ задана условием $g_k : x \mapsto (x \otimes k)^b$, где $b \in S(X)$, $k \in X$. К данному классу относятся XSL-алгоритмы блочного шифрования. Предположим существование такого разбиения $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$ множества X, что g_k сохраняет $\mathbf{W}$-разбиение для каждого $k \in X$, и $e \in W_0$. Так как $b \in S(X)$, то W_j — j-й смежный класс группы $(X, \otimes)$ по её подгруппе W_0, $j = 0, \ldots, r-1$. Справедливы включения

$$b \in IG_{\mathbf{W}},\ \langle g_k | k \in X\rangle \leqslant IG_{\mathbf{W}},\ \left\langle g_{k^{(1)}} \ldots g_{k^{(l)}} | (k^{(1)}, \ldots, k^{(l)}) \in X^l \right\rangle \leqslant IG_{\mathbf{W}}.$$

Очевидно, что существует бинарная операция $\odot$ на $\{0, \ldots, r-1\}$, удовлетворяющая равенству $W_i \otimes W_j = W_{i \odot j}$ для каждых $i, j \in \{0, \ldots, r-1\}$, где $i \odot j$ — номер смежного класса, содержащего произвольный представитель $\beta \in W_i \otimes W_j$. Заметим, что

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

Рассмотрим такое отображение $\varphi_{\mathbf{W}} : X \to \{0, \ldots, r-1\}$, что $\varphi_{\mathbf{W}} : \alpha \mapsto i$ тогда и только тогда, когда $\alpha \in W_i$, $i \in \{0, \ldots, r-1\}$. Ясно, что отображение $\varphi_{\mathbf{W}}$ задаёт гомоморфизм l-раундового алгоритма блочного шифрования с раундовой функцией

$g : X^2 \to X$ в l-раундовый алгоритм блочного шифрования с раундовой функцией $\bar{g} : \{0, \ldots, r-1\}^2 \to \{0, \ldots, r-1\}$, где

$$\bar{g}_{\varphi_{\mathbf{W}}(k)}\left(\varphi_{\mathbf{W}}(\alpha)\right) = \varphi_{\mathbf{W}}\left((\alpha \otimes k)^b\right) = \left(\varphi_{\mathbf{W}}(\alpha \otimes k)\right)^{\bar{b}} = \left(\varphi_{\mathbf{W}}(\alpha) \odot \varphi_{\mathbf{W}}(k)\right)^{\bar{b}} \qquad (1)$$

для каждых $(\alpha, k) \in X^2$. Заметим, что подстановка $\bar{b} \in S\left(\{0, \ldots, r-1\}\right)$ есть гомоморфный образ подстановки b.

Доказано, что $\mathbf{p}_{\mathbf{W}}(g) = \mathbf{p}(\bar{g})$, где $\mathbf{p}(\bar{g}) = (p_{\varepsilon,\lambda}(\bar{g}))$ — матрица вероятностей переходов разностей функции $\bar{g}$; $\mathbf{p}_{\mathbf{W}}(g)$ — матрица вероятностей переходов блоков разностей разбиения $\mathbf{W}$ функции g.

Определения $\otimes_{\mathbf{W},\mathrm{ch}}$-марковских алгоритмов блочного шифрования и $\otimes_{\mathbf{W},\mathrm{ch}}$-марковских преобразований приведены в [1].

Теорема 1. Пусть $l \in \mathbb{N}$, $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$ — разбиение множества X, $e \in W_0$, $W_0 < X$, W_j — j-й смежный класс группы $(X, \otimes)$ по её подгруппе W_0, $j = 0, \ldots, r-1$. Отображение $\varphi_{\mathbf{W}}$, определённое равенством (1), задаёт гомоморфизм l-раундового алгоритма блочного шифрования с раундовой функцией $g : X^2 \to X$, $g_k : x \mapsto (x \otimes k)^b$, в l-раундовый алгоритм блочного шифрования с раундовой функцией $\bar{g} : \{0, \ldots, r-1\}^2 \to \{0, \ldots, r-1\}$, $\bar{g}_\kappa : \beta \mapsto (\beta \odot \kappa)^{\bar{b}}$ тогда и только тогда, когда алгоритм блочного шифрования с раундовой функцией g является $\otimes_{\mathbf{W},\mathrm{ch}}$-марковским.

Заметим, что теорема 1 устанавливает соответствие между $\otimes_{\mathbf{W},\mathrm{ch}}$-марковостью и существованием гомоморфизма $\varphi_{\mathbf{W}}$ только для таких разбиений $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$, для которых W_j — j-й смежный класс группы $(X, \otimes)$ по её подгруппе W_0, $W_0 < X$. Однако класс $\otimes_{\mathbf{W},\mathrm{ch}}$-марковских алгоритмов шифрования и преобразований не ограничивается только такими разбиениями. Так, в [1] приведены $+_{\mathbf{W},\mathrm{ch}}$-марковские преобразования для аддитивной группы кольца вычетов $\mathbb{Z}_{2^n}$ для разбиений, отличных от приведённых в теореме 1.

Опишем ещё классы $\otimes_{\mathbf{W},\mathrm{ch}}$-марковских преобразований, не удовлетворяющих теореме 1. Для этого рассмотрим сначала классы $\otimes_{\mathbf{W},\mathrm{ch}}$-марковских аффинных преобразований для разбиений $\mathbf{W}$ $\mathbb{Z}_{2^m}$-модуля $\mathbb{Z}_{2^m}^d$.

Для $a \in \mathbb{Z}$ через $a_{(d)}$ обозначим такой наименьший элемент $a_{(d)} \in \{0, \ldots, d-1\}$, что $a_{(d)} \equiv a \pmod{d}$. Для $m, d \in \mathbb{N}$ и $\alpha = (\alpha_{d-1}, \ldots, \alpha_0) \in \mathbb{Z}_{2^m}^d$, $\beta = (\beta_{d-1}, \ldots, \beta_0) \in \mathbb{Z}_{2^m}^d$ положим

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

т. е. $+_{2^m}$ — операция покоординатного сложения в $\mathbb{Z}_{2^m}$-модуле $\mathbb{Z}_{2^m}^d$. Ясно, что при $m = 1$ выполняются равенства $d = n$, $\oplus = +_2$ и $V_n = \mathbb{Z}_2^n$.

Утверждение 1. Пусть $n = md$, $m, d \in \mathbb{N}$. Аффинное преобразование $h \in AGL_d(\mathbb{Z}_{2^m})$, где $h = (h_0, \lambda)$; $h : \alpha \mapsto \alpha^{h_0} +_{2^m} \lambda$; $h_0 \in GL_d\left(\mathbb{Z}_{2^m}\right)$; $\lambda \in \mathbb{Z}_{2^m}^d$, является $+_{2^m}\mathbf{W},\mathrm{ch}$-марковским для разбиения $\mathbf{W}$ $\mathbb{Z}_{2^m}$-модуля $\mathbb{Z}_{2^m}^d$ тогда и только тогда, когда h_0 сохраняет $\mathbf{W}$.

Из утверждения 1 следует, что преобразование h может являться $\oplus_{\mathbf{W},\mathrm{ch}}$-марковским и для разбиений $\mathbf{W}$ пространства V_n, блоки которых не являются смежными классами по некоторой подгруппе аддитивной группы V_n^+ векторного пространства V_n.

Приведём примеры примитивных групп $(AGL_n)_{\mathbf{W}}$ и соответствующих разбиений $\mathbf{W}$. Пусть $\Delta_j^{(n)}$ — множество всех векторов веса Хемминга $j \in \{0, \ldots, n\}$ из V_n; $\tilde{S}_n$ — группа подстановочных $(n \times n)$-матриц; $A\tilde{S}_n$ — аффинная подгруппа группы AGL_n,

подобная группе экспоненцирования $S_2 \uparrow S_n$. Стабилизатор $G_{\mathbf{0}}$ каждой не 2-транзитивной примитивной группы G, $A\tilde{S}_n \leqslant G \leqslant AGL_n$, сохраняет некоторое нетривиальное разбиение множества $V_n^\times$, блоками которого являются орбиты стабилизатора $G_{\mathbf{0}}$ на $V_n^\times$. Все такие разбиения описаны в [2], а классификация соответствующих групп — в [3, 4]. С применением теоремы 1, утверждения 1 и классификации надгрупп группы $A\tilde{S}_n$ описаны классы нелинейных $\oplus_{\mathbf{W},\mathrm{ch}}$-марковских преобразований для разбиений $\mathbf{W}$ пространства V_n, отличных от рассмотренных в теореме 1.

Очевидно, что $AGL_n = (AGL_n)_{\mathbf{W}}$ для $\mathbf{W} \in \left\{\{\Delta_0^{(n)}, V_n^\times\}, \{\alpha : \alpha \in V_n\}\right\}$.

Утверждение 2. Если 2-транзитивная группа $G < AGL_n$ такова, что $G_{\mathbf{0}}$ примитивна на $V_n^\times$, то $G \neq (AGL_n)_{\mathbf{W}}$ для каждого разбиения $\mathbf{W} \notin \left\{\{\Delta_0^{(n)}, V_n^\times\}, \{\{\alpha\} : \alpha \in V_n\}\right\}$.

В общем случае из $\oplus_{\mathbf{W},\mathrm{ch}}$-марковости преобразований $b_1, b_2 \in S(V_n)$ для некоторого разбиения $\mathbf{W}$ пространства V_n не следует $\oplus_{\mathbf{W},\mathrm{ch}}$-марковость преобразования $b_1 b_2$. Приведены условия на преобразования b_1, b_2, из которых вытекает $\oplus_{\mathbf{W},\mathrm{ch}}$-марковость преобразования $b_1 b_2$, а также условия того, что раундовая функция, задаваемая этими преобразованиями, является $\oplus_{\mathbf{W},\mathrm{ch}}$-марковской.

Пусть раундовая функция $g : V_n^2 \to V_n$ задана условием $g : (x, k) \mapsto (x \oplus k)^{sh}$, где $s = (s_{d-1}, \ldots, s_0) \in S(V_m)^d$, $h \in GL_n$. Приведены условия на h, при которых раундовая функция $g : (x, k) \mapsto (x \oplus k)^{sh}$ является $\oplus_{\mathbf{W},\mathrm{ch}}$-марковской для некоторого разбиения $\mathbf{W}$ пространства V_n.

ЛИТЕРАТУРА

1. *Погорелов Б. А., Пудовкина М. А.* $\otimes_{\mathbf{W},\mathrm{ch}}$-марковские преобразования // Прикладная дискретная математика. Приложение. 2015. № 8. С. 17–20.
2. *Музычук М. Е.* Подсхемы схемы Хемминга // Исследования по алгебраической теории комбинаторных объектов. ВНИИ системных исследований. Труды семинара. 1985. С. 49–76.
3. *Погорелов Б. А.* Подметрики метрики Хемминга и теорема А.А. Маркова // Труды по дискретной математике. 2006. № 9. С. 190–219.
4. *Погорелов Б. А., Пудовкина М. А.* Подметрики метрики Хемминга и преобразования, распространяющие искажения в заданное число раз // Труды по дискретной математике. 2007. № 10. С. 202–238.

УДК 510.52 DOI 10.17223/2226308X/8/26

О ГЕНЕРИЧЕСКОЙ СЛОЖНОСТИ ПРОБЛЕМЫ РАСПОЗНАВАНИЯ КВАДРАТИЧНЫХ ВЫЧЕТОВ[1]

А. Н. Рыбалов

Генерический подход к алгоритмическим проблемам предложен А. Мясниковым, И. Каповичем, П. Шуппом и В. Шпильрайном в 2003 г. В рамках этого подхода рассматривается поведение алгоритмов на множествах почти всех входов. В данной работе изучается генерическая сложность проблемы распознавания квадратичных вычетов в группах вычетов. Доказывается, что её естественная подпроблема генерически трудноразрешима (то есть трудна для почти всех входов) при условии, что проблема распознавания квадратичных вычетов трудноразрешима в классическом смысле.

[1]Работа поддержана грантом РФФИ № 15-41-04312.