УДК 519.7 DOI 10.17223/2226308X/15/4

О РАССЕИВАЮЩИХ СВОЙСТВАХ ОБОБЩЁННЫХ КВАЗИАДАМАРОВЫХ ПРЕОБРАЗОВАНИЙ НА КОНЕЧНЫХ АБЕЛЕВЫХ ГРУППАХ

Б. А. Погорелов, М. А. Пудовкина

Для произвольной конечной группы X предлагаются обобщения квазиадамаровых преобразований. При $X = \mathbb{Z}_{2^m}$ они включают в себя псевдоадамаровы преобразования алгоритмов блочного шифрования Safer, Safer+, Safer++, Twofish, а также квазиадамаровы преобразования, предложенные Х. Липмаа. Описаны свойства рассеивания биективными обобщёнными квазиадамаровыми преобразованиями систем импримитивности регулярных подстановочных представлений аддитивных групп $\mathbb{Z}_{2^m}^2$ и $\mathbb{Z}_{2^{2m}}$. Получены условия, при которых обобщённые квазиадамаровы преобразования максимально рассеивают все нетривиальные системы импримитивности этих двух групп.

Ключевые слова: *алгоритмы шифрования семейства Safer, алгоритм шифрования Twofish, псевдоадамарово преобразование, квазиадамарово преобразование, система импримитивности, примитивная группа, регулярное подстановочное представление.*

В ряде алгоритмов блочного шифрования (Safer [1], Hight [2], CS-Cipher [3], Speed [4] и др.) большинство преобразований, составляющих раундовую функцию, реализует побайтовую обработку блоков текста без взаимного влияния байтов с использованием абелевых групп. Наибольшее распространение среди таких «межбайтовых» преобразований получил класс псевдоадамаровых преобразований на двух байтах в алгоритмах семейства Safer. В [5] он обобщён до класса квазиадамаровых преобразований на аддитивных группах $\mathbb{Z}_{2^m}^2$, $\mathbb{Z}_2^{2m}$, для которых получены формулы нахождения элементов разностной матрицы. В [6] найден показатель рассеивания (branch number) тензорного произведения псевдоадамаровых преобразований алгоритма Safer.

Пусть $m \geqslant 2$; $(X, *)$ — конечная группа с бинарной операцией $*$; e — тождественная подстановка; $S(X)$ — симметрическая группа на X; $P(X) = \{b \mid b\colon X \to X\}$ — симметрическая полугруппа; $\alpha^g = \alpha g = g(\alpha)$ — образ элемента $\alpha \in X$ при действии на него преобразованием $g \in P(X)$;

$$\mathrm{Hom}(X) = \left\{v\colon X \to X \mid \forall x, y \in X \left(v(x * y) = v(x) * v(y)\right)\right\}.$$

Для алгоритмов блочного шифрования рассмотрим обобщение $h_{\bar\vartheta,\bar\psi}\colon X^2 \to X^2$ квазиадамаровых и псевдоадамаровых преобразований на группу $(X, *)$, которое задаётся набором отображений $\bar\vartheta = (\vartheta_1, \vartheta_2)$, $\bar\psi = (\psi_1, \psi_2)$, $\bar\vartheta, \bar\psi \in P(X)^2$б и условием

$$h_{\bar\vartheta,\bar\psi} : (\alpha_1, \alpha_2) \mapsto \left(\alpha_1^{\vartheta_1} * \alpha_2^{\vartheta_2}, \alpha_1^{\psi_1} * \alpha_2^{\psi_2}\right). \tag{1}$$

При

$$(X, *) \in \{(\mathbb{Z}_{2^m}, +), (\mathbb{Z}_2^m, \oplus)\},\ r_1, r_2 \in \{0, \ldots, m-1\}^2,$$
$$r_1 = (r_{11}, r_{12}),\ r_2 = (r_{21}, r_{22}),\ r_1 \neq r_2,\ \upsilon \in \{0, 1\}$$

квазиадамарово преобразование $u_{r_1,r_2}^{(\upsilon)}$ на X, введённое в [5], является частным случаем обобщения (1). Так, при $X = \mathbb{Z}_{2^m}$ оно задаётся условием

$$u_{r_1,r_2}^{(\upsilon)}\colon (\alpha_1, \alpha_2) \mapsto (2^{r_{11}}\alpha_1 + (-1)^{\upsilon}2^{r_{12}}\alpha_2, 2^{r_{21}}\alpha_1 + (-1)^{\upsilon}2^{r_{22}}\alpha_2)$$

и совпадает с $h_{\bar{\vartheta},\bar{\psi}}$ при следующих отображениях:

$$\vartheta_1\colon \alpha \mapsto 2^{r_{11}}\alpha \mod 2^m,\ \vartheta_2\colon \alpha \mapsto (-1)^v 2^{r_{12}}\alpha \mod 2^m,$$
$$\psi_1\colon \alpha \mapsto 2^{r_{21}}\alpha \mod 2^m,\ \psi_2\colon \alpha \mapsto (-1)^v 2^{r_{22}}\alpha \mod 2^m.$$

Отметим, что при чётном $r_{11} > 0$, $r_2 = (0,0)$ преобразование

$$u^{(0)}_{(r_{11},0),(0,0)}\colon (\alpha_1,\alpha_2) \mapsto (2^{r_{11}}\alpha_1 + \alpha_2, \alpha_1 + \alpha_2)$$

применено в хеш-функции FFT [7]. Кроме того, при $r_{11} = 1$ преобразование $u^{(0)}_{(r_{11},0),(0,0)}$, известное как псевдоадамарово, используется для улучшения рассеивающих свойств в алгоритмах блочного шифрования Safer, Safer+ [8], Safer++ [9] и Twofish [10]. В данной работе получены условия биективности преобразования $h_{\bar{\vartheta},\bar{\psi}}$. Так, для биективности $h_{\bar{\vartheta},\bar{\psi}}$ необходимо, чтобы одно из преобразований ϑ_1, ϑ_2, ψ_1, ψ_2 было биективным. Отсюда вытекает, что при $X = \mathbb{Z}_{2^m}$ биективное преобразование $h_{\bar{\vartheta},\bar{\psi}}$ принимает вид

$$h_{\bar{\vartheta},\bar{\psi}}\colon (\alpha_1,\alpha_2) \mapsto \left(\alpha_{v_1}^{\vartheta_{v_1}} + b_1\alpha_{v_2},\ a\cdot\alpha_{v_1}^{\vartheta_{v_1}} + b_2\alpha_{v_2}\right) \text{ для всех } (\alpha_1,\alpha_2) \in \mathbb{Z}_{2^m}^2, \tag{2}$$

где $\{v_1,v_2\} = \{1,2\}$, $v_2 = v_1(1,2)$, $\vartheta_{v_1} \in S(\mathbb{Z}_{2^m})$, $a, b_1, b_2 \in \mathbb{Z}_{2^m}$, причём

$$b_2 - a\cdot b_1 \equiv 1 \,(\mathrm{mod}\ 2). \tag{3}$$

В работе показывается, что условию (2) удовлетворяет биективное квазиадамарово преобразование.

Для импримитивной группы $G \leqslant S(X)$ с системой импримитивности $\overline{W}$ (т. е. $\overline{W}$ — нетривиальное разбиение множества X на равномощные блоки, сохраняемое группой G) рассеивание подстановкой $g \in S(X)$ системы $\overline{W}$, а также расстояние от g до G будем характеризовать посредством матрицы $c^{(\overline{W})}(g)$, введённой в [11]. Разбиению $\overline{W} = \{W_0,\dots,W_{p-1}\}$ множества X и подстановке $g \in G$ ставится в соответствие матрица $c^{(\overline{W})}(g) = \left[c^{(\overline{W})}_{i,j}(g)\right]$, где

$$c^{(\overline{W})}_{i,j}(g) = |W_i^g \cap W_j|,\ W_i^g = \{\beta^g \mid \beta \in W_i\},\ i,j \in \{0,\dots,p-1\}.$$

Для группы $(G,*)$ рассмотрим её правое подстановочное представление $\varphi_G\colon G \to S(G)$, заданное условием

$$\varphi_G(k)\colon x \mapsto x * k \ \text{ для всех } \ x,k \in G.$$

Пусть $\bar{G} = \varphi_G(G) = \{\varphi_G(k) \mid k \in G\}$. Для $d \in \{0,\dots,2m\}$, $t \in \{0,\dots,d\}$ положим $\overline{W}^{(d,t)} = \left\{W_0^{(d,t)},\dots,W_{2^t-1}^{(d,t)}\right\}$, где

$$W_i^{(d,t)} = \left\{j \equiv i \,(\mathrm{mod}\ 2^t) \mid j \in \mathbb{Z}_{2^d}\right\},\ i = 0,\dots,2^t-1.$$

Легко видеть, что $\overline{W}^{(d,1)},\dots,\overline{W}^{(d,d-1)}$ — нетривиальные системы импримитивности группы $\bar{\mathbb{Z}}_{2^d}$.

Для $t_1,t_2 \in \{0,\dots,m\}$ положим

$$W_{i,j}^{(m,t_1,t_2)} = W_i^{(m,t_1)} \times W_j^{(m,t_2)},\ i = 0,\dots,2^{t_1}-1,\ j = 0,\dots,2^{t_2}-1,$$
$$\overline{W}^{(m,t_1,t_2)} = \left\{W_{i,j}^{(m,t_1,t_2)} \mid i \in \{0,\dots,2^{t_1}-1\}, j \in \{0,\dots,2^{t_2}-1\}\right\}.$$

В работе описываются свойства рассеивания преобразованием $h_{\bar{\vartheta},\bar{\psi}}$ систем импримитивности регулярных подстановочных представлений $\bar{\mathbb{Z}}_{2^m}^2 = \bar{\mathbb{Z}}_{2^m} \times \bar{\mathbb{Z}}_{2^m}$ и $\bar{\mathbb{Z}}_{2^{2m}}$ соответственно двух групп наложения ключа $\mathbb{Z}_{2^m}^2$ и $\mathbb{Z}_{2^{2m}}$.

Легко видеть, что группа $\bar{\mathbb{Z}}_{2^m}^2$ импримитивна, а $\left\{\overline{W}^{(m,t_1,t_2)} \mid t_1, t_2 \in \{0,\ldots,m\}\right\}$ — множество всех её систем импримитивности. Найдены элементы матрицы $c^{(\overline{W}^{(m,t,t)})}(h_{\bar{\vartheta},\bar{\psi}})$ для преобразования $h_{\bar{\vartheta},\bar{\psi}}$ и системы импримитивности $\overline{W}^{(m,t,t)}$ для каждого $t \in \in \{0,\ldots,m\}$.

Утверждение 1. Пусть преобразование $h_{\bar{\vartheta},\bar{\psi}}\colon \mathbb{Z}_{2^m}^2 \to \mathbb{Z}_{2^m}^2$ удовлетворяет условиям (2) и (3), $v_1 = 1$, $\vartheta_1 \in S(\mathbb{Z}_{2^m})$. Группа $\left\langle h_{\bar{\vartheta},\bar{\psi}}, \bar{\mathbb{Z}}_{2^m}^2 \right\rangle \leqslant S(\mathbb{Z}_{2^m}^2)$ является примитивной тогда и только тогда, когда примитивна группа $\left\langle \vartheta_1, \bar{\mathbb{Z}}_{2^m} \right\rangle \leqslant S(\mathbb{Z}_{2^m})$.

Нетривиальной системой импримитивности группы $\bar{\mathbb{Z}}_{2^{2m}}$ является $\overline{W}^{(2m,t)}$ для каждого $t \in \{1,\ldots,2m-1\}$. Преобразование $h_{\bar{\vartheta},\bar{\psi}}$, заданное условием (1), зависит от элемента $v_1 \in \{1,2\}$.

Утверждение 2. Пусть $t \in \{1,\ldots,2m-1\}$, преобразование $h_{\bar{\vartheta},\bar{\psi}}\colon \mathbb{Z}_{2^m}^2 \to \mathbb{Z}_{2^m}^2$ удовлетворяет условиям (2) и (3), $v_1 = 1$, $a \equiv 1 \pmod 2$, $\vartheta_1 \in S(\mathbb{Z}_{2^m})$. Тогда для каждых $j_1, j_2 \in \{0,\ldots,2^t-1\}$ элементы матрицы $c^{\left(\overline{W}^{(2m,t)}\right)}\left(h_{\bar{\vartheta},\bar{\psi}}\right)$ удовлетворяют следующим свойствам:

1) $c_{j_1,j_2}^{\left(\overline{W}^{(2m,t)}\right)}\left(h_{\bar{\vartheta},\bar{\psi}}\right) = 2^{2m-2t}$, если $t \in \{1,\ldots,m\}$;
2) $c_{j_1,j_2}^{\left(\overline{W}^{(2m,t)}\right)}\left(h_{\bar{\vartheta},\bar{\psi}}\right) \in \{0,1\}$, если $t \in \{m+1,\ldots,2m-1\}$.

Следовательно, матрица $c^{\left(\overline{W}^{(2m,t)}\right)}\left(h_{\bar{\vartheta},\bar{\psi}}\right)$ является «максимально равномерной» для каждого $t \in \{1,\ldots,2m-1\}$, а преобразование $h_{\bar{\vartheta},\bar{\psi}}$ максимально удалено от группы $\mathrm{IG}_{\overline{W}^{(2m,t)}}$, которая состоит из всех подстановок, сохраняющих систему импримитивности $\overline{W}^{(2m,t)}$. Поэтому преобразование $h_{\bar{\vartheta},\bar{\psi}}$ максимально рассеивает все нетривиальные системы импримитивности группы $\bar{\mathbb{Z}}_{2^{2m}}$. Показано также, что при чётном a матрица $c^{\left(\overline{W}^{(2m,t)}\right)}\left(h_{\bar{\vartheta},\bar{\psi}}\right)$ не является «максимально равномерной». Схожие результаты получены для $v_1 = 2$. Таким образом, введённый класс обобщённых квазиадамаровых преобразований существенно шире классов псевдоадамаровых и квазиадамаровых преобразований, причём он содержит преобразования, которые отличны от квазиадамаровых, но также обладают хорошими рассеивающими свойствами.

ЛИТЕРАТУРА

1. *Massey J. L.* SAFER K-64: a byte-oriented block-ciphering algorithm // FSE 1994. LNCS. 1994. V. 1267. P. 1–17.
2. *Hong D., Sung J., Hong S., et al.* A new block cipher suitable for low-resource device // CHES 2006. LNCS. 2006. V. 4249. P. 46–59.
3. *Stern J. and Vaudenay S.* CS-Cipher // FSE 1998. LNCS. 1998. V. 1372. P. 189–204.
4. *Zheng Y.* The SPEED cipher // Financial Cryptography. LNCS. 1997. V. 1318. P. 71–89.
5. *Lipmaa H.* On differential properties of pseudo-Hadamard transform and related mappings // INDOCRYPT 2002. LNCS. 2002. V. 2551. P. 48–61.
6. *St Denis T.* Fast Pseudo-Hadamard Transforms. Cryptology ePrint Archive, Report 2004/010. 2004. `https://eprint.iacr.org/2004/010.pdf`.
7. *Schnorr C.-P.* FFT-Hash II, efficient cryptographic hashing // EUROCRYPT'92. LNCS. 1992. V. 658. P. 45–54.

8. *Massey J., Khachatrian G., and Kuregian M.* Nomination of SAFER+ as Candidate Algorithm for the Advanced Encryption Standard (AES). NIST AES Proposal, 1998. `http://www.princeton.edu/~rblee/safer+/`.
9. *Massey J., Khachatrian G., and Kuregian M.* Nomination of SAFER++ as Candidate Algorithm for NESSIE. 2003. `https://www.cosic.esat.kuleuven.be/nessie/workshop/submissions/safer++.zip`.
10. *Schneier B., Kelsey J., Whiting D., et al.* The Twofish Encryption Algorithm: A 128-Bit Block Cipher. N.Y.: John Wiley & Sons, 1999.
11. *Погорелов Б. А., Пудовкина М. А.* О расстояниях от подстановок до импримитивных групп при фиксированной системе импримитивности // Дискретная математика. 2013. Т. 25. № 3. С. 78–95.