# ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

DOI 10.17223/20710410/8/1

УДК 519.95

## НЕОБХОДИМЫЕ И ДОСТАТОЧНЫЕ УСЛОВИЯ ТРИВИАЛЬНОСТИ ЛИНЕЙНОЙ СТРУКТУРЫ МОНОМИАЛЬНОГО ОТОБРАЖЕНИЯ НАД ПОЛЕМ ИЗ $2^{2^t}$ ЭЛЕМЕНТОВ

А. Н. Алексейчук, Р. В. Проскуровский

*Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт», г. Киев, Украина*

**E-mail:** alex-crypto@mail.ru, roman-crypto@mail.ru

В терминах двоичного представления натурального числа $d$ получены необходимые и достаточные условия, при которых все ненулевые линейные комбинации координатных функций отображения $x \mapsto x^d$, $x \in \mathbf{GF}(2^{2^t})$, не имеют линейных трансляторов.

**Ключевые слова:** *линейная структура дискретного отображения, конечное поле, мономиальное отображение.*

Одним из известных требований к дискретным отображениям, используемым в современных симметричных криптосистемах, является условие отсутствия линейных трансляторов. Напомним (см., например, [1]), что ненулевой вектор $a \in \{0,1\}^n$ называется линейным транслятором отображения $\varphi : \{0,1\}^n \to \{0,1\}^m$, если существует элемент $c \in \{0,1\}^m$, такой, что равенство $\varphi(x \oplus a) \oplus \varphi(x) = c$ выполняется для всех $x \in \{0,1\}^n$. Как правило, наличие линейных трансляторов (или, как говорят, нетривиальность линейной структуры) отображения $\varphi$ свидетельствует о его криптографических слабостях.

Исследованию строения множества линейных трансляторов булевых функций и подстановок на множестве $\{0,1\}^n$ посвящены работы [2–5] и др. В [6] предложено обобщение понятия линейного транслятора для отображений векторных пространств над конечными полями и исследованы распределения ряда числовых характеристик множества линейных трансляторов случайных равновероятных отображений указанного вида. В [7] описаны биективные преобразования конечных модулей над конечным ассоциативным кольцом с единицей, имеющие заданное непустое множество линейных трансляторов.

С криптографической точки зрения более естественным (и более жестким) является требование, состоящее в отсутствии линейных трансляторов не только у данного отображения $\varphi : \{0,1\}^n \to \{0,1\}^m$, но и у всех ненулевых линейных комбинаций его координатных функций. Формализация этого условия (применительно к более широкому классу отображений одной конечной абелевой группы в другую) приводит к понятию тривиальности линейной структуры дискретного отображения, введенному в работе [8]. Отметим, что это, более общее по сравнению с [6, 7], понятие возникает естественным образом при обосновании достаточных условий стойкости блочных шифров относительно алгебраических атак, основанных на гомоморфизмах (см. [8, 9]).

**Определение** [8]. Пусть $G_1$ и $G_2$ — конечные абелевы группы, $\varphi : G_1 \to G_2$ — произвольное отображение. Будем говорить, что $\varphi$ *имеет тривиальную линейную структуру*, если не существует элемента $a \in G_1 \setminus \{0\}$ и комплексного характера $\psi \neq 1$ группы $G_2$, таких, что функция $\psi(\varphi(x+a) - \varphi(x))$, $x \in G_1$, является константой.

В [10] получены достаточные условия тривиальности линейной структуры преобразований аддитивной группы конечного поля и показано, что при $n = 2^t$, $t \geqslant 2$, тривиальную линейную структуру имеет отображение $\varphi(x) = x^{2^n-2}$, $x \in \mathbf{GF}(2^n)$, используемое при построении узлов замены современных блочных шифров [11, 12].

Полное описание полиномов над конечными полями, задающих отображения с тривиальной линейной структурой, представляет собой непростую задачу. В настоящей работе исследуются мономиальные отображения над полем порядка $2^{2^t}$.

Введем следующие обозначения:
$F = \mathbf{GF}(2^n)$, $n = 2^t$, $t \geqslant 2$;
$F^* = F \setminus \{0\}$;
$\mathrm{Tr}(x) = x + x^2 + ... + x^{2^{n-1}}$ — абсолютный след элемента $x \in F$;
$\overline{i,j} = \{l \in \mathbb{Z} : i \leqslant l \leqslant j\}$, $i, j \in \mathbb{Z}$.

Пусть $l = \sum\limits_{i=0}^{n-1} 2^i l_i$ — двоичное представление числа $l \in \overline{0,\, 2^n - 1}$. Обозначим $I_l = \{i \in \overline{0, n-1} : l_i = 1\}$. Для любых $M \subseteq \overline{0, n-1}$, $i \in \overline{0, n-1}$, $l \in \overline{0,\, 2^n - 1}$ положим

$$M + i = \{(j + i) (\mathrm{mod}\, n) : j \in M\},\ s(l, i) = 2^i l (\mathrm{mod}(2^n - 1)).$$

Непосредственно из данных определений вытекает следующее утверждение.

**Лемма 1.** Для любых $i \in \overline{0, n-1}$, $l \in \overline{0,\, 2^n - 1}$ справедливо равенство

$$I_{s(l,i)} = I_l + i.$$

Сформулируем два вспомогательных утверждения, первое из которых является следствием условия $n = 2^t$ и теоремы 2.39, приведенной в [13], а второе следует из данного выше определения и известных свойств конечных полей (см. теоремы 5.7 и 2.21 в [13]).

**Лемма 2.** Для любого $x \in F$ элементы $x, x^2, ..., x^{2^{n-1}}$ образуют базис поля $F$ над полем $\mathbf{GF}(2)$ тогда и только тогда, когда $\mathrm{Tr}(x) = 1$.

**Лемма 3.** Отображение $\varphi : F \to F$ тогда и только тогда имеет тривиальную линейную структуру, когда для любых $a, b \in F^*$ выполняется соотношение $\mathrm{Tr}(b\varphi(x+a) + b\varphi(x)) \neq \mathrm{const}$. При этом отображения $x \mapsto \varphi(x)$ и $x \mapsto \varphi(x^2)$, $x \in F$, имеют тривиальную или нетривиальную линейную структуру одновременно.

Сформулируем и докажем теорему, содержащую необходимые и достаточные условия тривиальности линейной структуры мономиального отображения

$$\varphi(x) = x^d,\ x \in F. \tag{1}$$

Отметим, что на основании второго утверждения леммы 3 можно ограничиться случаем нечетных значений $d$.

**Теорема.** Пусть $d \in \overline{3, 2^n - 2}$, $d \equiv 1 (\mathrm{mod}\, 2)$. Тогда отображение (1) имеет тривиальную линейную структуру в том и только том случае, когда существует множество $M \subseteq \overline{0, n-1}$, $M \notin \{\varnothing, I_d\}$, такое, что

$$\left|\{i \in \overline{0, n-1} : M + i \subseteq I_d\}\right| \equiv 1 (\mathrm{mod}\, 2). \tag{2}$$

***Доказательство.*** Пусть $a, b \in F^*$; тогда для любого $x \in F$

$$b(\varphi(x+a)+\varphi(x)) = b((x+a)^d + x^d) = ba^d((z+1)^d + z^d),$$

где $z = xa^{-1}$. Отсюда на основании лемм 2 и 3 вытекает, что $\varphi$ имеет тривиальную линейную структуру в том и только в том случае, когда

$$\exists\, z \in F^* \left(\mathrm{Tr}((z+1)^d + z^d) = 1\right). \tag{3}$$

Действительно, согласно лемме 2, при выполнении условия (3) множество $\{(z+1)^d + z^d : z \in F\}$ содержит некоторый базис поля $F$ над полем $\mathbf{GF}(2)$, откуда следует, что равенство $\mathrm{Tr}(b(\varphi(x+a)+\varphi(x))) = \mathrm{const}$, $x \in F$, возможно лишь при условии $ba^d = 0$. Наоборот, если $\mathrm{Tr}((z+1)^d + z^d) = 0$ для любого $z \in F^*$, то в силу равенства $\mathrm{Tr}(1) = n \cdot 1 = 0$ справедливо соотношение $\mathrm{Tr}(\varphi(x+1)+\varphi(x))) = 0$, $x \in F$, означающее, что отображение $\varphi$ имеет нетривиальную линейную структуру.

Используя определение функции след и равенство $\mathrm{Tr}(1) = 0$, получим

$$\mathrm{Tr}((z+1)^d + z^d) = \mathrm{Tr}\left(\sum_{j=1}^{d-1} z^j \binom{d}{j}\right) = \sum_{j=1}^{d-1}\sum_{i=0}^{n-1} \binom{d}{j} z^{j\cdot 2^i},$$

откуда на основании тождества $z^{2^n-1} = 1$, $z \in F^*$, вытекает следующее равенство:

$$\mathrm{Tr}((z+1)^d + z^d) = \sum_{i=0}^{2^n-2} A_l z^l,\ z \in F^*, \tag{4}$$

где

$$A_l = \sum_{\substack{(i,\,j):\\ i\in\overline{0,\,n-1},j\in\overline{1,\,d-1},\\ j\cdot 2^i \equiv l \bmod (2^n-1)}} \binom{d}{j},\ l \in \overline{0,\,2^n-2}. \tag{5}$$

Поскольку полином от $z$ в правой части равенства (4) имеет степень, меньшую $2^n$, то условие (3) равносильно следующему условию:

$$\exists\, l \in \overline{0,\,2^n-2}\ \ (A_l \neq 0). \tag{6}$$

Преобразуем выражение (5). Заметим, что сравнение $j2^i \equiv l \bmod(2^n-1)$ равносильно сравнению $j \equiv 2^{n-i}l \bmod(2^n-1)$; следовательно,

$$A_l = \sum_{\substack{i\in\overline{0,\,n-1}:\\ s(l,\,i)\in\overline{1,\,d-1}}} \binom{d}{s(l,i)},\ l \in \overline{0,\,2^n-2}. \tag{7}$$

Далее, по теореме Лукаса [14] $\binom{d}{s(l,\,i)} \equiv 1 (\mathrm{mod}\, 2)$ тогда и только тогда, когда множество единичных разрядов в двоичном представлении числа $s(l,\,i)$ содержится во множестве $I_d$, то есть $I_{s(l,\,i)} \subseteq I_d$. При этом, согласно лемме 1, $I_{s(l,\,i)} = I_l + i$, $i \in \overline{0,\,n-1}$, $l \in \overline{0,\,2^n-2}$. Отсюда на основании формулы (7) вытекает, что $A_l = 0$, если $l = 0$ или $|I_l| \geqslant |I_d|$. Таким образом, условие (6) равносильно следующему условию:

$$\exists\, l \in \overline{0,\,2^n-2}\ (|I_l| < |I_d|\ \&\ A_l \neq 0). \tag{8}$$

Заметим, наконец, что для любого $l \in \overline{1,\,2^n-2}$, такого, что $|I_l| < |I_d|$, справедлива импликация

$$\forall\, i \in \overline{0,\,n-1}\ \left[\binom{d}{s(l,\,i)} \equiv 1 (\mathrm{mod}\, 2)\ \Rightarrow\ s(l,\,i) \in \overline{1,\,d-1}\right].$$

Следовательно, для указанных $l$

$$A_l = \sum_{i=0}^{n-1} \binom{d}{s(l,i)} \equiv \left|\{i \in \overline{0,\, n-1} : I_l + i \subseteq I_d\}\right| (\mathrm{mod}\, 2). \qquad (9)$$

Теперь нетрудно завершить доказательство теоремы. Если отображение (1) имеет тривиальную линейную структуру, то на основании соотношений (8) и (9) множество $M = I_l \notin \{\oslash, I_d\}$ удовлетворяет условию (2).

Наоборот, пусть множество $M \subseteq \overline{0, n-1}$, $M \notin \{\oslash, I_d\}$, удовлетворяет условию (2). Тогда $M = I_l$ для некоторого $l \in \overline{1,\, 2^n - 1} \setminus \{d\}$ и существует $i \in \overline{0,\, n-1}$, такое, что $I_l + i \subseteq I_d$. Следовательно, $|I_l| < |I_d|$, в частности, $l \neq 2^n - 1$. Отсюда на основании соотношений (2) и (9) вытекает справедливость условия (8). Таким образом, отображение (1) имеет тривиальную линейную структуру, что и требовалось доказать. ■

Отметим, что полученный критерий тривиальности линейной структуры отображений вида (1) допускает простую практическую проверку.

**Следствие 1.** Если в условиях теоремы двоичное представление числа $d$ содержит нечетное число единиц, то отображение (1) имеет тривиальную линейную структуру.

Для доказательства достаточно рассмотреть множество $M = \{0\}$.

**Следствие 2.** Пусть в условиях теоремы $d = 4^k - 2^k + 1$, $k \equiv 1 (\mathrm{mod}\, 2)$, $k \geqslant 3$. Тогда отображение (1) (известное как функция Касами; см. [1], с. 340) имеет тривиальную линейную структуру.

Для доказательства достаточно положить $M = \{0, 1, 2\}$ и воспользоваться соотношением $\left|\{i \in \overline{0,\, n-1} : M + i \subseteq I_d\}\right| = k - 2 \equiv 1 (\mathrm{mod}\, 2)$.

## ЛИТЕРАТУРА


1. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 470 с.
2. *Evertse J. H.* Linear structures in blockciphers // Advances in Cryptology — EUROCRYPT'87. Springer Verlag, 1988. P. 249–266.
3. *Lai X.* Additive and linear structures of cryptographic functions // Fast Software Encryption — FSE'94. Springer Verlag, 1995. P. 75–86.
4. *Ященко В. В.* О критерии распространения для булевых функций и о бент-функциях // Проблемы передачи информации. 1997. Т. 33. № 1. С. 75–86.
5. *Dawson E., Wu Ch. K.* On the linear structures of symmetric functions // Australian J. of Combinatorics. Springer Verlag, 1997. V. 16. P. 239–243.
6. *Сачков В. Н.* Трансляторы и трансляции дискретных функций // Труды по дискретной математике. М.: Гелиос АРВ, 2006. Т. 9. С. 253–268.
7. *Пудовкина М. А.* Линейные структуры групп подстановок над конечным модулем // Прикладная дискретная математика. 2008. № 1. С. 25–28.
8. *Алексейчук А. Н.* Достаточные условия стойкости рандомизированных блочных систем шифрования относительно метода криптоанализа на основе коммутативных диаграмм // Реєстрація, зберігання і обробка даних. 2007. Т. 9. № 2. С. 61–68.
9. *Алексейчук А. Н.* Критерий примитивности группы подстановок, порожденной раундовыми преобразованиями Rijndael-подобного блочного шифра // Реєстрація, зберігання і обробка даних. 2004. Т. 6. № 2. С. 11–18.

10. *Алексейчук А. Н., Скрынник Е. В.* Классы отображений с тривиальной линейной структурой над конечным полем // Реєстрація, зберігання і обробка даних. 2008. Т. 10. № 3. С. 80–88.
11. *Daemen J., Rijmen D.* AES proposal: Rijndael // `htpp://csrc.nist.gov/encription/aes/rijndael/Rijndael.pdf`.
12. *Aoki A., Ichikawa T., Kanda M., et al.* Camellia: a 128-bit block cipher suitable for multiple platforms — Design and Analysis // Selected Areas in Cryptography. Springer Verlag, 2001. P. 39–56.
13. *Лидл Р., Нидеррайтер Г.* Конечные поля. М.: Мир, 1988. Т. 1, 2. 818 с.
14. *Берлекэмп Э.* Алгебраическая теория кодирования. М.: Мир, 1971. 477 с.