

ТРАНСЛЯТОРЫ И ТРАНСЛЯЦИИ ДИСКРЕТНЫХ ФУНКЦИЙ

В. Н. САЧКОВ

Даны некоторые обобщения понятий аддитивного и линейного трансляторов. Получены необходимые и достаточные условия того, что подпространство размерности r пространства V_n над полем $\mathbf{GF}(q)$ является подпространством линейных трансляторов функции $f: V_n \rightarrow V_m$. Найдено рекуррентное соотношение, оценки и асимптотическая формула для числа таких функций. Аналогичные результаты получены для функций, имеющих аддитивные трансляторы, образующие подпространство, а также для подстановок пространства V_n . Для случайных функций и случайных подстановок установлены точные и предельные распределения для числа (a, b) -трансляций относительно группы G .

§ 1. ВВЕДЕНИЕ

Пусть p — простое, s и t — натуральные числа, s делит t , $\mathbf{GF}(p^t)$ — поле Галуа и $\mathbf{GF}(p^s)$ — подполе поля $\mathbf{GF}(p^t)$. Рассмотрим векторные пространства V_n и V_m над полями $\mathbf{GF}(p^s)$ и $\mathbf{GF}(p^t)$, имеющие размерности n и m соответственно, и пусть функция f задает отображение

$$f: V_n \rightarrow V_m. \quad (1.1)$$

Ненулевой элемент $a \in V_n$ называется аддитивным транслятором функции f , если для всех $x \in V_n$

$$f(x + a) = f(x) + b, \quad (1.2)$$

где $b = f(a) - f(0)$.

Ненулевой элемент $a \in V_n$ называется линейным транслятором функции f , если для всех $x \in V_n$ и любого $c \in \mathbf{GF}(p^s)$

$$f(x + ca) = f(x) + cb, \quad (1.3)$$

где $b = f(a) - f(0)$.

Имеют место следующие свойства трансляторов.

Свойство 1.1. Множество всех аддитивных трансляторов функции f вместе с нулевым элементом образует аддитивную подгруппу V_n .

Свойство 1.2. Если пространство V_n задано над простым полем $\mathbf{GF}(p)$, то множество всех аддитивных трансляторов функции f вместе с нулевым элементом образует подпространство пространства V_n .

Свойство 1.3. Множество всех линейных трансляторов функции f вместе с нулевым элементом образует подпространство пространства V_n .

Отметим, что свойство 1.2 является следствием свойства 1.3, так как если пространство V_n задано над простым полем $\mathbf{GF}(p)$, то аддитивный транслятор является одновременно и линейным транслятором.

Доказательства свойств 1.1, 1.2 и 1.3 вытекают непосредственно из их определения. Отметим только, что при доказательстве свойства 1.1 используется соотношение

$$f(a + a') = f(a) + f(a') - f(0),$$

где a и a' — аддитивные трансляторы функции f . В доказательствах свойств 1.2 и 1.3 используется равенство

$$f(ca) = cf(a) - (c - 1)f(0),$$

где a — либо аддитивный, либо линейный транслятор, а $c \in \mathbf{GF}(p)$, или $c \in \mathbf{GF}(p')$, соответственно. При этом используется тот факт, что любой линейный транслятор является также и аддитивным транслятором функции f .

Для случая $s = t$ определения аддитивного и линейного трансляторов и их свойства, являющиеся аналогами свойств 1.1 и 1.3, приведены в статье [1]. В этой же статье установлено, что если подпространство $W_r \subseteq V_n$ линейных трансляторов функции f имеет размерность r , то существует невырожденное линейное преобразование переменных, в результате применения которого

функцию f можно представить в виде суммы линейной функции от r переменных и некоторой функции от $n - r$ переменных.

В статье [2] приведен пример, показывающий, что при $s = t$ для аддитивных трансляторов такое представление функций возможно только в том случае, если оба пространства V_n и V_m заданы над простым полем $\mathbf{GF}(p)$, т. е. $s = t = 1$.

Понятия аддитивного и линейного трансляторов, как предложенные в статье [1], так и их обобщения в данной работе, представляют интерес для изучения криптографических свойств дискретных функций, заданных в виде отображений векторных пространств над полями Галуа. Эти свойства используются при построении методов криптоанализа поточных и блочных шифрсистем, в частности метода дифференциалов и линейного метода.

Приведем основные результаты, полученные в данной работе.

В § 2 рассматриваются функции вида (1.1), где V_n и V_m — векторные пространства размерностей n и m над полем $\mathbf{GF}(q)$, $q = p^t$, p — простое, t — натуральное числа. Получены необходимые и достаточные условия того, что подпространство $W_r \subseteq V_n$ размерности r является подпространством всех линейных трансляторов с условием максимальности функции f . С использованием этих условий найдено рекуррентное соотношение для числа $N_r(n, m, q)$ функций, имеющих подпространство линейных трансляторов размерности r , $1 \leq r \leq n$. Для $N_r(n, m, q)$ получены неравенства и асимптотическая формула при n , $(n - r) \rightarrow \infty$.

В § 3 рассматриваются функции вида (1.1), где V_n и V_m — пространства размерности n и m над полями $\mathbf{GF}(p)$ и $\mathbf{GF}(q)$, $q = p^t$, соответственно. Установлены необходимые и достаточные условия того, что подпространство $W_r \subseteq V_n$ размерности r является подпространством всех аддитивных трансляторов функции f . Для числа $N_r(n, m, p)$ функций, имеющих подпространство аддитивных трансляторов с условием максимальности размерности r , получено рекуррентное соотношение, а также оценки и асимптотическая формула при n , $(n - r) \rightarrow \infty$.

В § 4 для функций, имеющих как аддитивные, так и линейные трансляторы, дана характеристика с использованием систем уравнений, решением которых является функция f .

Даны необходимые и достаточные условия того, что подпространство $W_r \subseteq V_n$ размерности r является подпространством

линейных трансляторов подстановки $f: V_n \rightarrow V_n$. Из этих условий выводится рекуррентное соотношение для числа $M_r(n, q)$ подстановок, для которых подпространство линейных трансляторов имеет размерность r , $1 \leq r \leq n$. Для $M_r(n, q)$ найдены оценки и асимптотическая формула при n , $(n - r) \rightarrow \infty$.

В § 5 рассматриваются вероятностные распределения числа (a, b) -трансляции относительно группы $G \subseteq V_n$ для случайных функций и случайных подстановок. Для случайных функций распределение является биномиальным и его предельное поведение определяется величиной $\alpha_{nm} = (n - m(p^l - 1))t - l$, где p^l , $1 \leq l \leq t$, — порядок группы G . Для случайных подстановок, представляющих интерес для криптографии, найдены точные и предельные распределения для числа (a, b) -трансляций относительно группы G . Установлено, что предельные распределения вырожденные, за исключением случая $l = 1$, $p = 2$, когда предельным является закон Пуассона с параметром $\lambda = 1/2$.

§ 2. ЛИНЕЙНЫЕ ТРАНСЛЯТОРЫ

Пусть W_r — подпространство V_n , имеющее базис a_1, a_2, \dots, a_r , \bar{W}_{n-r} — дополнение W_r в пространстве V_n , имеющее базис $a_{r+1}, a_{r+2}, \dots, a_n$. Тогда $a_1, a_2, \dots, a_r, a_{r+1}, \dots, a_n$ — базис пространства V_n , и V_n представимо в виде прямой суммы $V_n = W_r + \bar{W}_{n-r}$. Будем говорить, что подпространство линейных трансляторов функции f вида (1.1) обладает свойством максимальности, если оно содержит все линейные трансляторы этой функции. Дадим необходимые и достаточные условия того, что подпространство W_r пространства V_n является подпространством линейных трансляторов со свойством максимальности. Необходимость условий фактически доказана в статье [1].

ТЕОРЕМА 1. *Подпространство $W_r \subseteq V_n$ является подпространством линейных трансляторов со свойством максимальности для функции f вида (1.1) тогда и только тогда, когда функция f представима в виде*

$$f(x_1 a_1 + \dots + x_n a_n) = x_1(f(a_1) - f(0)) + \dots + x_r(f(a_r) - f(0)) + f(x_{r+1} a_{r+1} + \dots + x_n a_n), \quad (2.1)$$

где $f(x_{r+1} a_{r+1} + \dots + x_n a_n)$ — сужение функции f на подпространстве \bar{W}_{n-r} , не имеющее линейных трансляторов, и представление (2.1) имеет место для всех x , $x \in \mathbf{GF}(q)$, $1 \leq i \leq n$.

Если W_r — подпространство линейных трансляторов функции f со свойством максимальности, то представление (2.1) получается индукцией по r из соотношения (1.3). Если линейно не зависящий от a_1, a_2, \dots, a_r элемент $a = \alpha_{r+1}a_{r+1} + \dots + \alpha_n a_n \in \bar{W}_{n-r}$ является линейным транслятором функции $f(x_{r+1}a_{r+1} + \dots + x_n a_n)$, $\alpha_i \in \mathbf{GF}(q)$, $r+1 \leq i \leq n$, то элемент $a + 0 \in V_n$ является линейным транслятором функции f . Это противоречит свойству максимальности подпространства W_r .

Пусть теперь $W_r \subseteq V_n$ — подпространство, для которого функция f с использованием значений на элементе $0 \in V_n$, базисных элементах $a_1, a_2, \dots, a_r \in W_r$ и значений на \bar{W}_{n-r} имеет представление вида (2.1). Тогда для любого элемента $a = \alpha_1 a_1 + \dots + \alpha_r a_r \in W_r$, $\alpha_i \in \mathbf{GF}(q)$, $1 \leq i \leq r$, сужение функции f на W_r имеет вид

$$f(\alpha_1 a_1 + \dots + \alpha_r a_r) = \alpha_1(f(a_1) - f(0)) + \dots + \alpha_r(f(a_r) - f(0)) + f(0).$$

С использованием этого равенства находим, что для любого $x = x_1 a_1 + \dots + x_n a_n \in V_n$, $x_i \in \mathbf{GF}(q)$, $1 \leq i \leq n$, и любого $c \in \mathbf{GF}(q)$

$$f(x + ca) = f(x) + c(f(a) - f(0)).$$

Это означает, что $W_r \subseteq W$, где W — подпространство всех линейных трансляторов функции f . Допустим, что существует линейный транслятор $a' \notin W_r$ для функции f и, значит, a' линейно не зависит от a_1, a_2, \dots, a_r . Следовательно, $a' = 0 + \tilde{a}$, где \tilde{a} — линейный транслятор сужения функции f на подпространстве \bar{W}_{n-r} . Это противоречит условию теоремы, стало быть $W = W_r$.

Обозначим через $F(W_r)$ множество всех функций вида (1.1), для которых W_r является подпространством линейных трансляторов размерности r с условием максимальности. В силу теоремы 1 такое множество определено для любого подпространства размерности r , и любая функция из этого множества имеет представление (2.1). Выбор конкретной функции $f \in F(W_r)$ определяется выбором значений $f(0), f(a_1), \dots, f(a_r)$ и заданием сужения f на подпространстве \bar{W}_{n-r} , не имеющего линейных трансляторов.

СЛЕДСТВИЕ 1. Если W_r и $\tilde{W}_{\tilde{r}}$ — различные подпространства пространства V_n , то

$$F(W_r) \cap F(\tilde{W}_{\tilde{r}}) = \emptyset. \tag{2.2}$$

Допустим, что существует функция $f \in F(W_r) \cap F(\tilde{W}_{\tilde{r}})$, для которой W_r и $\tilde{W}_{\tilde{r}}$ — подпространство линейных трансляторов с условием максимальности.

Так как $W_r \neq \tilde{W}_{\tilde{r}}$, то существует элемент $a \in \tilde{W}_{\tilde{r}} \setminus W_r \cap \tilde{W}_{\tilde{r}}$, который является линейным транслятором f , не принадлежащим W_r . Это противоречит условию максимальности W_r .

Из теоремы 1 и следствия 1 вытекает следствие 2, определяющее способ вычисления количества функций вида (1.1), для которых подпространство линейных трансляторов с условием максимальности имеет заданную размерность.

СЛЕДСТВИЕ 2. Пусть $N_r(n, m, q)$ — число функций $f: V_n \rightarrow V_m$, для которых подпространство линейных трансляторов с условием максимальности имеет размерность r . Тогда для любых $m \leq n$ имеет место рекуррентное соотношение

$$N_r(n, m, q) = \begin{bmatrix} n \\ r \end{bmatrix}_q q^{m(r+1)} \left\{ q^{mq^{n-r}} - \sum_{k=1}^{n-r} N_k(n-r, m, q) \right\},$$

$$r = 1, 2, \dots, n-1, \quad (2.3)$$

где $\begin{bmatrix} n \\ r \end{bmatrix}_q$ — коэффициент Гаусса, равный числу подпространств размерности r в пространстве V_n и вычисляемый по формуле

$$\begin{bmatrix} n \\ r \end{bmatrix}_q = \frac{(q^n - 1)(q^{n-1} - 1) \dots (q^{n-r+1} - 1)}{(q^r - 1)(q^{r-1} - 1) \dots (q - 1)}. \quad (2.4)$$

Начальные условия определяются равенствами

$$N_r(n, m, q) = q^{m(r+1)}, \quad r = 1, 2, \dots, n. \quad (2.5)$$

В соответствии с представлением функции f , удовлетворяющей условиям теоремы 1 вида (2.1), и следствием 1 величина $N_r(n, m, q)$ равна произведению трех величин: числа способов выбора в V_n подпространств размерности r , являющихся подпространствами линейных трансляторов функции f с условием максимальности, числа способов выбора значений $f(0), f(a_1), \dots, f(a_r)$, определяющих линейную часть в представлении f вида (2.1), и числа способов выбора сужений f на подпространстве \tilde{W}_{n-r} , не имеющих линейных трансляторов.

С использованием рекуррентного соотношения (2.3), начальных условий (2.5) и формулы (2.4) получаем выражение для

$N_r(n, m, q)$ при $n = 1, 2, 3$:

$$\begin{aligned} N_1(1, m, q) &= q^{2m}, \\ N_1(2, m, q) &= (q + 1)q^{2m}(q^{qm} - q^{2m}), \\ N_2(2, m, q) &= q^{3m}, \\ N_1(3, m, q) &= (q^2 + q + 1)q^{2m}(q^{mq^2} - (q - 1)q^{2m}(q^{qm} - q^{2m}) - q^{3m}), \\ N_2(3, m, q) &= (q^2 + q + 1)q^{3m}(q^{qm} - q^{2m}), \\ N_3(3, m, q) &= q^{4m}. \end{aligned} \tag{2.6}$$

С использованием формул (2.6) из рекуррентного соотношения (2.3) можно получить выражение для $N_r(4, m, q)$, $1 \leq r \leq 4$.

С помощью этого выражения, формул (2.6) и соотношения (2.3) вычисляются значения $N_r(n, m, q)$ для $n - 4 \leq r \leq n$. Для оценки значений $N_r(n, m, q)$ при $1 \leq r \leq n - 5$ можно использовать следующие неравенства:

$$\begin{aligned} \left[\begin{matrix} n \\ r \end{matrix} \right]_q q^{m(q^{n-r} + r + 1)} (1 - R_{n-r}(n, m, q)) &\leq N_r(n, m, q) \leq \\ &\leq \left[\begin{matrix} n \\ r \end{matrix} \right]_q q^{m(q^{n-r} + r + 1)}, \quad r = 1, 2, \dots, n - 5, \end{aligned} \tag{2.7}$$

в которых $R_{n-r}(n, m, q)$ оценивается с использованием неравенств

$$\begin{aligned} \theta R_{n-r}(n, m, q) q^{m(q^{n-r} - q^{n-r-1} - 2) - (n-r)^2/4} &\leq \\ &\leq \begin{cases} C_0, & (n - r) \text{ четно,} \\ C_1, & (n - r) \text{ нечетно,} \end{cases} \end{aligned} \tag{2.8}$$

где

$$\theta = \prod_{j=1}^{\infty} \left(1 - \frac{1}{q^j} \right), \tag{2.9}$$

$$C_0 = \sum_{j=-\infty}^{\infty} q^{-j^2}, \quad C_1 = \sum_{j=-\infty}^{\infty} q^{-(j-1/2)^2}. \tag{2.10}$$

Справедливость верхней оценки в (2.7) очевидна. Используя эту верхнюю оценку, получаем, что

$$R_{n-r}(n, m, q) \leq \sum_{k=1}^{n-r} \left[\begin{matrix} n - r \\ k \end{matrix} \right]_q q^{-m(q^{n-r} - q^{n-r-k} - k - 1)}. \tag{2.11}$$

Отсюда следует, что

$$R_{n-r}(n, m, q) \leq G_{n-r} q^{-m(q^{n-r} - q^{n-r-1} - 2)}, \quad (2.12)$$

где G_n — числа Гауа, определяемые равенством

$$G_n = \sum_{r=0}^n \left[\begin{matrix} n \\ r \end{matrix} \right]_q. \quad (2.13)$$

Из формулы (2.4) получаем:

$$\left[\begin{matrix} n \\ r \end{matrix} \right]_q = q^{r(n-r)} \frac{\prod_{j=n-r+1}^n \left(1 - \frac{1}{q^j}\right)}{\prod_{j=1}^r \left(1 - \frac{1}{q^j}\right)}, \quad r = 1, 2, \dots, n. \quad (2.14)$$

Следовательно,

$$\left[\begin{matrix} n \\ r \end{matrix} \right]_q \leq \frac{q^{r(n-r)}}{\theta}, \quad r = 1, 2, \dots, n, \quad (2.15)$$

и при $n, (n-r) \rightarrow \infty$

$$\left[\begin{matrix} n \\ r \end{matrix} \right]_q = \frac{q^{r(n-r)}}{\prod_{j=1}^r \left(1 - \frac{1}{q^j}\right)} (1 + o(1)).$$

Из равенства (2.13) и оценки (2.15) получаем, что

$$\theta q^{-(n-r)^2/4} G_{n-r} \leq \begin{cases} C_0, & (n-r) \text{ четно,} \\ C_1, & (n-r) \text{ нечетно.} \end{cases} \quad (2.16)$$

Теперь оценка (2.8) следует из неравенств (2.12) и (2.16).

СЛЕДСТВИЕ 3. Если $n \rightarrow \infty$ и $(n-r) \rightarrow \infty$, то имеет место асимптотическая формула

$$N_r(n, m, q) = \frac{q^{m(q^{n-r} + r + 1) + r(n-r)}}{\prod_{j=1}^r \left(1 - \frac{1}{q^j}\right)} \left(1 + O\left(\frac{1}{q^{n-r}}\right)\right), \quad r = 1, 2, \dots \quad (2.17)$$

Формула (2.17) следует из неравенств (2.7), оценки (2.8) и формул (2.5).

§ 3. АДДИТИВНЫЕ ТРАНСЛЯТОРЫ

Пусть $\mathbf{GF}(p)$ — простое подполе поля $\mathbf{GF}(q)$, $q = p^t$, $\mathbf{GF}(p) = \{0, 1, \dots, p-1\}$, и V_n и V_m — векторные пространства размерностей n и m над полями $\mathbf{GF}(p)$ и $\mathbf{GF}(q)$ соответственно. Для функции f вида (1.2) обозначим через W_r подпространство пространства V_n всех аддитивных трансляторов, имеющее размерность r . Пусть a_1, a_2, \dots, a_r — базис W_r , \bar{W}_{n-r} — дополнение W_r в пространстве V_n , имеющее базис $a_{r+1}, a_{r+2}, \dots, a_n$, и $a_1, \dots, a_r, a_{r+1}, \dots, a_n$ — базис пространства V_n , представимого в виде прямой суммы.

ТЕОРЕМА 2. *Подпространство $W_r \subseteq V_n$ является подпространством аддитивных трансляторов со свойством максимальности для функции f вида (1.2) тогда и только тогда, когда функция f представима в виде*

$$f(x_1 a_1 + \dots + x_n a_n) = x_1(f(a_1) - f(0)) + \dots + x_r(f(a_r) - f(0)) + f(x_{r+1} a_{r+1} + \dots + x_n a_n), \quad (3.1)$$

где $f(x_{r+1} a_{r+1} + \dots + x_n a_n)$ — сужение функции f на подпространстве \bar{W}_{n-r} , не имеющее аддитивных трансляторов, и представление (3.1) имеет место для всех $x_i \in \mathbf{GF}(p)$, $1 \leq i \leq n$.

Доказательство теоремы 2 аналогично доказательству теоремы 1.

Пусть $F(W_r)$ — множество всех функций вида (3.1), для которых $W_r, W'_r \subseteq V_n$ являются подпространствами аддитивных трансляторов с условием максимальности размерностей r и r' соответственно. Тогда

$$F(W_r) \cap F(W'_r) = \emptyset, \quad (3.2)$$

если $W_r \neq W'_r$.

Из теоремы 2 и равенства (3.2) для числа $N_r(n, m, p)$ функций вида (1.2), имеющих подпространство аддитивных трансляторов с условием максимальности размерности r , получаем рекуррентное соотношение

$$N_r(n, m, p) = \begin{bmatrix} n \\ r \end{bmatrix}_p q^{m(r+1)} \left\{ q^{mp^{n-r}} - \sum_{k=1}^{n-r} N_k(n-r, m, p) \right\}, \quad (3.3)$$

$$r = 1, 2, \dots, n-1,$$

с начальным условием

$$N_r(n, m, p) = q^{m(r+1)}, \quad q = p^t, \quad r = 1, 2, \dots, n. \quad (3.4)$$

Из соотношения (3.3) вытекают неравенства

$$\begin{aligned} \left[\begin{matrix} n \\ r \end{matrix} \right]_p q^{m(p^{n-r}+r+1)}(1 - R_{n-r}(n, m, p)) &\leq N_r(n, m, p) \leq \\ &\leq \left[\begin{matrix} n \\ r \end{matrix} \right]_p q^{m(q^{n-r}+r+1)}, \end{aligned} \quad (3.5)$$

причем

$$\begin{aligned} \tilde{\theta} q^{m(p^{n-r}-p^{n-r-1}-2)p^{(n-r)^2/4}} R_{n-r}(n, m, p) &\leq \\ &\leq \begin{cases} \tilde{C}_0, & (n-r) \text{ четно,} \\ \tilde{C}_1, & (n-r) \text{ нечетно,} \end{cases} \end{aligned} \quad (3.6)$$

где

$$\begin{aligned} \theta &= \prod_{j=1}^{\infty} \left(1 - \frac{1}{p^j} \right), \\ \tilde{C}_0 &= \sum_{j=-\infty}^{\infty} p^{-j^2}, \quad \tilde{C}_1 = \sum_{j=-\infty}^{\infty} p^{-(j-1/2)^2}. \end{aligned}$$

Из неравенств (3.5) при $n, (n-r) \rightarrow \infty$ следует асимптотическая формула

$$N_r(n, m, p) = \frac{q^{m(q^{n-r}+r+1)} p^{r(n-r)}}{\prod_{j=1}^r \left(1 - \frac{1}{p^j} \right)} \left(1 + O\left(\frac{1}{p^{n-r}} \right) \right). \quad (3.7)$$

Доказательства соотношений (3.3), (3.5), (3.6) и (3.7) аналогичны доказательствам соответствующих соотношений (2.3), (2.7), (2.8) и (2.17).

Отметим, что если при $q = p^t$ рассматривать поле $\mathbf{GF}(q)$ как линейное пространство размерности t над простым полем $\mathbf{GF}(p)$, а функцию $f: V_n \rightarrow V_m$ как отображение пространства $\mathbf{GF}(p)^{nt}$ в пространство $\mathbf{GF}(q)^m$, то для таких функций аддитивные трансляторы совпадают с линейными трансляторами и, стало быть, вместе с нулевым элементом образуют подпространство $\mathbf{GF}(p)^{nt}$. Вместе с тем, аддитивные трансляторы $f: V_n \rightarrow V_m$ в общем случае образуют только подгруппу V_n .

§ 4. АДДИТИВНЫЕ И ЛИНЕЙНЫЕ ТРАНСЛЯТОРЫ И СИСТЕМЫ УРАВНЕНИЙ ДЛЯ ФУНКЦИЙ

Рассмотрим такие подстановки L_a и L_b , определяемые элементами $a \in V_n$ и $b \in V_m$, действующие на пространствах V_n и V_m над полем $\mathbf{GF}(q)$ соответственно, что

$$L_a(x) = x + a, \quad L_b(y) = y + b \quad (4.1)$$

для всех $x \in V_n$, $y \in V_m$. Подстановки L_a и L_b регулярны и содержат p^{nt-1} и p^{mt-1} циклов длины p соответственно, $q = p^t$.

Очевидны следующие два свойства.

Свойство 4.1. Ненулевой элемент $a \in V_n$ является аддитивным транслятором функции $f: V_n \rightarrow V_m$ тогда и только тогда, когда f является решением уравнения

$$L_a f = f L_b, \quad b = f(a) - f(0). \quad (4.2)$$

Свойство 4.2. Ненулевой элемент $x \in V_n$ является линейным транслятором функции $f: V_n \rightarrow V_m$ тогда и только тогда, когда f является решением системы уравнений

$$L_{c_i a} f = f L_{c_i b}, \quad i = 1, 2, \dots, q-1, \quad (4.3)$$

где $b = f(a) - f(0)$, $\mathbf{GF}(q) = \{0, c_1, \dots, c_{q-1}\}$.

Из свойства 4.2 вытекает следующая теорема.

ТЕОРЕМА 3. Подпространство $W_r \subseteq V_n$ с базисом a_1, a_2, \dots, a_r является подпространством линейных трансляторов с условием максимальности функции $f: V_n \rightarrow V_m$ тогда и только тогда, когда f является решением системы уравнений

$$\begin{aligned} L_{c_i a_j} f &= f L_{c_i b_j}, \quad b_j = f(a_j) - f(0), \\ i &= 1, 2, \dots, q-1, \quad j = 1, 2, \dots, r, \end{aligned} \quad (4.4)$$

причем, если существует такое $a' \in V_n$, что $L_{a'} f = f L_{b'}$, $b' = f(a') - f(0)$, то a' линейно выражается через a_1, a_2, \dots, a_r .

Если W_r — подпространство линейных трансляторов с условием максимальности функции f , то для любого $a = x_1 a_1 + \dots + x_r a_r \in W_r$, $x_i \in \mathbf{GF}(q)$, $1 \leq i \leq r$, имеет место система равенств

$$L_{x_1 a_1 + \dots + x_r a_r} f = f L_{x_1 b_1 + \dots + x_r b_r}, \quad x_i \in \mathbf{GF}(q), \quad 1 \leq i \leq r, \quad (4.5)$$

из которой следует, что функция f является решением системы (4.4).

Пусть теперь W_r — подпространство V_n с базисом a_1, a_2, \dots, a_r и для системы (4.3) существует решение f . В соответствии со свойством 4.2 элементы базиса a_1, a_2, \dots, a_r являются линейными трансляторами f . Отсюда и из свойств умножения подстановок L_a и L_b следует выполнение равенств (4.5). Это означает, что любой элемент $a \in W_r$ является линейным транслятором f . Допустим, что существует $a' \notin W_r$, являющийся линейным транслятором f . Тогда f удовлетворяет уравнению $L_{a'}f = fL_{b'}$, $b' = f(a') - f(0)$. Следовательно, a' линейно выражается через элементы a_1, a_2, \dots, a_r , что противоречит условию теоремы.

ТЕОРЕМА 4. Подпространство $W_r \subseteq V_n$ над полем $\mathbf{GF}(p)$ с базисом a_1, a_2, \dots, a_r является подпространством аддитивных трансляторов с условием максимальности функции $f: V_n \rightarrow V_n$ тогда и только тогда, когда f является решением системы уравнений

$$L_{a_j}f = fL_{b_j}, \quad b_j = f(a_j) - f(0), \quad j = 1, 2, \dots, r, \quad (4.6)$$

причем, если существует такое $a' \notin V_n$, что $L_{a'}f = fL_{b'}$, $b' = f(a') - f(0)$, то a' линейно выражается через a_1, a_2, \dots, a_r .

Доказательство теоремы 4 аналогично доказательству теоремы 3.

Отметим, что рассмотрение структуры решений систем (4.4) и (4.6) позволяет для функции f установить свойства (2.1) и (3.1) соответственно.

Рассмотрим теперь аддитивные и линейные трансляторы подстановок

$$f: V_n \rightarrow V_n, \quad (4.7)$$

где V_n — векторное пространство размерности n над полем $\mathbf{GF}(q)$.

Свойство 4.3. Элемент $a \in V_n$ является аддитивным (линейным) транслятором подстановки f вида (4.7) тогда и только тогда, когда $b = f(a) - f(0)$ есть аддитивный (линейный) транслятор подстановки f^{-1} .

Свойство 4.3 непосредственно следует из свойств 4.1 и 4.2.

ТЕОРЕМА 5. Подпространство $W_r \subseteq V_n$ с базисом a_1, a_2, \dots, a_r является подпространством линейных трансляторов с условием максимальности для подстановки $f: V_n \rightarrow V_n$ тогда и только тогда, когда векторы $f(a_1) - f(0), f(a_2) - f(0), \dots, f(a_r) -$

$-f(0)$ образуют базис подпространства $U_r \subseteq V_n$ линейных трансляторов подстановки f^{-1} со свойством максимальности.

Из свойств 4.2 и 4.3 следует, что если a_1, a_2, \dots, a_r — базис подпространства W_r линейных трансляторов подстановки f и $b_i = f(a_i) - f(0)$, $1 \leq i \leq r$, то b_1, b_2, \dots, b_r являются линейными трансляторами подстановки f^{-1} . Из линейной независимости a_1, a_2, \dots, a_r следует линейная независимость b_1, b_2, \dots, b_r . Следовательно, b_1, b_2, \dots, b_r порождают подпространство U_r линейных трансляторов функции f^{-1} . Свойство максимальности U_r вытекает из свойства максимальности W_r . В свою очередь, если b_1, b_2, \dots, b_r — базис подпространства линейных трансляторов с условием максимальности подстановки f^{-1} , то a_1, a_2, \dots, a_r линейно независимы и порождают подпространство W_r линейных трансляторов f .

Пусть $M_r(n, q)$ — число подстановок $f: V_n \rightarrow V_n$, для которых подпространство линейных трансляторов с условием максимальности имеет размерность r .

Тогда из соотношения (2.1) и линейной независимости $f(a_1) - f(0), \dots, f(a_r) - f(0)$ следует рекуррентное соотношение

$$M_r(n, q) = \left[\begin{matrix} n \\ r \end{matrix} \right]_p q^{n(r+1)} \prod_{j=n-r+1}^n \left(1 - \frac{1}{q^j} \right) \left\{ (q^{n-r})! - \sum_{k=1}^{n-r} M_k(n-r, q) \right\},$$

$$r = 1, 2, \dots, n-1, \tag{4.8}$$

с начальными условиями

$$M_r(r, q) = q^{r(r+1)} \prod_{j=1}^r \left(1 - \frac{1}{q^j} \right), \quad r = 1, 2, \dots, n. \tag{4.9}$$

Из соотношения (4.8) и начальных условий (4.9) имеем:

$$M_{n-1}(n, q) = \left[\begin{matrix} n \\ 1 \end{matrix} \right]_q q^{n^2} \prod_{j=2}^n \left(1 - \frac{1}{q^j} \right) \{q! - q(q-1)\},$$

$$M_{n-2}(n, q) = \left[\begin{matrix} n \\ 2 \end{matrix} \right]_q q^{n(n-1)} \prod_{j=3}^n \left(1 - \frac{1}{q^j} \right) \times$$

$$\times \{(q^2)! - (q+1)q^2(q^2-1)(q! - q(q-1)) - q^3(q-1)(q^2-1)\}.$$

Аналогичным образом вычисляются значения $M_r(n, q)$ для $1 \leq r \leq n - 3$.

Из соотношения (4.8), оценок (2.15) и

$$M_r(n, q) \leq \frac{1}{\theta} q^{r(n-r)+(r+1)n} (q^{n-r})!, \quad r = 1, 2, \dots, n, \quad (4.10)$$

получаем неравенства

$$\begin{aligned} \left[\begin{matrix} n \\ r \end{matrix} \right]_q q^{n(r+1)} \prod_{j=n-r+1}^n \left(1 - \frac{1}{q^j} \right) (q^{n-r})! \{1 - R_{n-r}(q)\} &\leq M_r(n, q) \leq \\ &\leq \left[\begin{matrix} n \\ r \end{matrix} \right]_q q^{n(r+1)} \prod_{j=n-r+1}^n \left(1 - \frac{1}{q^j} \right) (q^{n-r})!, \end{aligned} \quad (4.11)$$

где

$$R_{n-r}(q) \leq \frac{1}{\theta} \sum_{k=1}^{n-r} q^{k(n-r-k)+(k+1)(n-r)} \frac{(q^{n-r-k})!}{(q^{n-r})!}. \quad (4.12)$$

Используя формулу Стирлинга, из (4.12) получаем оценку

$$\begin{aligned} R_{n-r}(q) &\leq \frac{1}{\theta} q^{(n-r)^2} \left(\frac{e}{q^{n-r}} \right)^{q^{n-r-1}(q-1)} \times \\ &\times \left(1 + \sum_{k=1}^{n-r-1} \frac{1}{q^{kq^{n-r-k} - (n-r)}} \right). \end{aligned} \quad (4.13)$$

Если $n \rightarrow \infty$ и $(n-r) \rightarrow \infty$, то из неравенств (4.11) и (4.13) находим, что

$$\begin{aligned} M_r(n, q) &= \frac{\sqrt{2\pi} (q^{n-r}/e)^{q^{n-r}}}{r \prod_{j=1}^r \left(1 - \frac{1}{q^j} \right)} q^{(r+1/2)(n-r)+n(r+1)} (1 + o(1)), \\ & \quad r = 1, 2, \dots \end{aligned} \quad (4.14)$$

§ 5. ТРАНСЛЯЦИИ СЛУЧАЙНЫХ ФУНКЦИЙ

Пусть G — подгруппа аддитивной группы поля $\mathbf{GF}(p^t)$, имеющая порядок $|G| = p^l$, $1 \leq l \leq t$.

Для элемента $a \in V_n$ рассмотрим аддитивную подгруппу aG пространства V_n над полем $\mathbf{GF}(p^t)$. Аддитивную группу V_n раз-

ложим на смежные классы по подгруппе aG :

$$V_n = aG \cup (x_1 + aG) \cup \dots \cup (x_{p^{nt-l}-1} + aG).$$

Для функции $f: V_n \rightarrow V_m$ (a, b) -трансляцией относительно группы G будем называть элемент x из любого смежного класса $(x_k + aG)$, $0 \leq k \leq p^{p^{nt-l}} - 1$, $x_0 = 0$, если

$$F(x + ga) = f(x) + gb$$

для любого элемента $g \in G$.

В частности, если $G = \mathbf{GF}(p)$, то (a, b) -трансляцию f будем называть аддитивной. Если $G = \mathbf{GF}(p^t)$, то (a, b) -трансляция называется линейной.

Для случайной равновероятной функции $f: V_n \rightarrow V_m$ случайная величина $\xi_{nm}^{(l)}(p^t)$, равная числу (a, b) -трансляций относительно группы G , имеет биномиальное распределение с параметрами $(p^{nt-l}, p^{-mt(p^l-1)})$, где p^{nt-l} — число испытаний, $p^{-mt(p^l-1)}$ — вероятность успеха в каждом испытании.

Для аддитивных и линейных (a, b) -трансляций эти параметры имеют вид $(p^{nt-l}, p^{-mt(p^l-1)})$ и $(p^{(n-1)t}, p^{-mt(p^t-1)})$ соответственно.

В соответствии с классическими результатами предельные распределения биномиального распределения при $n, m \rightarrow \infty$ зависят от поведения величины $\alpha_{nm} = (n - m(p^l - 1))t - l$:

- а) при $\alpha_{nm} \rightarrow \infty$ случайная величина $\xi_{nm}^{(l)}(p^t)$ при стандартных нормировках имеет в пределе нормальное распределение с параметрами $(0, 1)$;
- б) при $\alpha_{nm} \rightarrow \alpha$, $|\alpha| < \infty$, предельным является распределение Пуассона с параметром $\lambda = p^\alpha$;
- в) при $\alpha_{nm} \rightarrow -\infty$ предельное распределение вырождено.

В частности, для $\xi_{nn}^{(1)}(2)$ предельным является закон Пуассона с параметром $\lambda = 1/2$. За исключением случая $l = 1, p = 2, t = 1$ предельное распределение $\xi_{nn}^{(l)}(p^t)$ является вырожденным.

Для случайной булевой функции от n переменных $p = 2, m = l = t = 1$. Следовательно, $\lambda_{n1} = n - 2$ и предельное распределение является нормальным.

Для случайной равновероятной подстановки $f: V_n \rightarrow V_n$ биномиальные моменты случайной величины $\eta_{nn}^{(l)}(p^t)$, равной числу

(a, b)-трансляций относительно группы G , имеют следующий вид:

$$B_k^{(l)}(n, p^t) = \frac{1}{k!} \frac{(p^{nt-l})_k (p^{nt})_k}{(p^{nt})_{kp^t}}, \quad k = 0, 1, \dots, p^{nt-l}.$$

Соответствующее точное распределение определяется формулами

$$\mathbf{P}(\eta_{nn}^{(l)}(p^t) = r) = \sum_{k=r}^{p^{nt-l}} (-1)^{k-r} \binom{k}{r} B_k^{(l)}(n, p^t), \quad r = 0, 1, \dots, p^{nt-1}.$$

Для любого фиксированного k при $n \rightarrow \infty$ имеет место следующее асимптотическое представление:

$$B_k^{(l)}(n, p^t) = \frac{1}{k!} (p^{(2-p^l)nt-l})^k (1 + o(1)), \quad k = 0, 1, \dots$$

Из этого представления вытекает следующая теорема.

ТЕОРЕМА 6. При $n \rightarrow \infty$ случайная величина $\eta_{nn}^{(l)}(p^t)$ имеет в качестве предельного распределения распределение Пуассона с параметром $\lambda = 1/2$ тогда и только тогда, когда $l = 1$, $p = 2$. При любых других значениях параметров l и p предельное распределение является вырожденным.

Данная теорема определяет условия выбора функций, обладающих необходимыми криптографическими свойствами.

В заключение выражаю признательность профессору М. М. Глухову за полезное обсуждение работы.

СПИСОК ЛИТЕРАТУРЫ

1. Lai X. Additive and linear structures of cryptographic functions. — In: Fast Software Encryption. — Berlin: Springer, 1994, p. 75–85.
2. Nyberg K. On construction of highly nonlinear permutations. — EUROCRYPT'92, 1993, p. 92–98.
3. Глухов М.М., Сачков В.Н. О некоторых задачах теории дискретных функций, представляющих интерес для криптографии. — Конференция по теоретической кибернетике, посвященная памяти С. В. Яблонского. Тезисы доклада. — М., 2004.
4. Шилов Г.Е. Математический анализ. Конечномерные линейные пространства. — М.: Наука, 1969.