

# 1 Весовые характеристики функции. Сбалансированная функция. Теорема о связи множества всех отображений декартовой степени конечного множества с множеством всех систем координатных функций, следствие. Система весовых характеристик системы функций. Нормальное весовое строение системы функций. Критерий сбалансированности системы функций, следствие.

Функция  $f : X \rightarrow Y$  сбалансирована, если

$$|\{x \in X \mid f(x) = y\}| = |\{x \in X \mid f(x) = z\}| \quad \forall y, z \in Y. \quad (1)$$

**Теорема:**

$$\varphi : X^n \rightarrow X^m \iff F_{m,n} = \{f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\} \quad (2)$$

где  $F_{m,n}$  - система координатных функций.

**Следствие:** Множество всех отображений  $V_n \rightarrow V_m$  взаимно однозначно соответствует множеству всех систем из  $m$  б.ф. от  $n$  переменных.

Весовые характеристики:

$$N_{r_1, \dots, r_s}^{i_1, \dots, i_s} = |\{(x_1, \dots, x_n) \in X^n \mid f_{i_1}(x_1, \dots, x_n) = r_1, \dots, f_{i_s}(x_1, \dots, x_n) = r_s\}| \quad (3)$$

где  $\{i_1, \dots, i_s\} \subseteq \{1 \dots m\}$ ,  $(r_1, \dots, r_s) \in X^s$ . Множество весовых характеристик функции образуют систему весовых характеристик этой функции.

Функция имеет нормальное весовое строение (н.в.с.), если  $(X = E_k - \text{числа от } 0 \text{ до } k-1 \text{ (типа } \mathbb{Z}_k))$ :

$$N_{r_1, \dots, r_s}^{i_1, \dots, i_s} = k^{n-s} \quad (4)$$

**Теорема:** Отображение  $F_{m,n}$  сбалансировано  $\iff F_{m,n}$  имеет н.в.с.

**Следствие 1:** Отображение, заданное системой б.ф.  $F_{m,n}$ , сбалансировано  $\iff$  для любого непустого подмножества  $\{i_1, \dots, i_s\}$  мн-ва  $\{1, \dots, m\}$ :

$$|f_{i_1}(x_1, \dots, x_n) \cdot \dots \cdot f_{i_s}(x_1, \dots, x_n)| = 2^{n-s} \quad (5)$$

**Следствие 2:** Если  $F_{m,n}$  сбалансировано, то все его координатные ф-ции тоже сбалансированы.

## 2 Алгебраически зависимая система функций. Критерий алгебраической зависимости системы функций, следствие (без доказательства). Линейные, аффинные, нелинейные функции векторных пространств, замечания. Критерий сбалансированности линейного отображения векторных пространств (без доказательства).

Система ф-ций  $F_{m,n}$  является АЗ, если  $\exists b \in X$  и  $\exists \psi : X^m \rightarrow X$ , отличная от константы, для которых

$$\psi(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)) \equiv b \quad (6)$$

**Теорема:** Отображение  $\varphi$ , определяемое системой  $F_{m,n}$ , сюръективно  $\iff F_{m,n}$  - АНЗ

**Следствие:** Преобразование  $g$  множества  $X^n$  биективно  $\iff$  АНЗ система его координатных ф-ций.

Пусть  $P$  - некоторое поле. Ф-ция  $\varphi : P^n \rightarrow P^m$  линейная, если:

$$\forall x, y \in P^n \quad \forall a, b \in P : \varphi(a \cdot x + b \cdot y) = a \cdot \varphi(x) + b \cdot \varphi(y) \quad (7)$$

Ф-ция  $\varphi : P^n \rightarrow P^m$  аффинная, если:

$$\varphi(x) = \psi(x) + a \quad (8)$$

где  $\psi$  - линейная функция,  $a \in P^m$

Ф-ция, отличная от аффинной, называется нелинейной.

**Утверждение:** Между мн-вом линейных функций из  $P^n$  в  $P^m$   $\varphi$  и мн-вом матриц  $m \times n$   $M_\varphi$  существует биекция. При этом коэф-ты линейного полинома  $i$ -й координатной функции соответствуют  $i$ -й строке матрицы  $M_\varphi$ . Верно следующее:  $\varphi$  сбалансирована  $\iff \text{rang} M_\varphi = m$ .

## 3 Треугольное преобразование декартовой степени конечно-го множества. Критерий биективности треугольного преобразования, следствие. Отображение неавтономного (преобразование автономного) регистра сдвига над конечным множеством. Линейные регистры сдвига. Критерий биективности преобразования автономного регистра сдвига, следствие.

Преобразование  $g_n$  множества  $X^n$  называется треугольным, если  $g_n = F_{\Delta,n} = \{f_1(x_1), f_2(x_1, x_2), \dots, f_n(x_1, \dots, x_n)\}$ , иначе если  $S(f_i) \subseteq 1, \dots, i$  для  $i = 1, \dots, n$ , где  $S(f)$  — множество номеров существенных переменных функции  $f$ .

**Теорема:** Треугольное преобразование  $g_n$  множества  $X^n$  биективно  $\iff$  функция  $f_i(x_1, \dots, x_i)$  биективна по последней переменной  $x_i$ ,  $i = 1, \dots, n$ .

Пусть  $\tau(y_1, y_2)$  — внутренняя бинарная операция на  $X$ . Отображение  $f\varphi : X^{n+1} \rightarrow X^n$  называется **отображением неавтономного регистра левого сдвига над  $X$  с обратной связью**  $f : X^n \rightarrow X$ , если

$$f\varphi(x_1, \dots, x_n, x_{n+1}) = (x_2, \dots, x_n, \tau(f(x_1, \dots, x_n), x_{n+1})). \quad (9)$$

То есть,  $x_{n+1}$  нам приходит извне. Мы считаем значение функции  $\tau$  от текущих элементов регистра и от новой пришедшей переменной, и ставим его на последнее (самое правое, т.к. регистр левого сдвига  $\Rightarrow$  всё сдвигается влево) место.

- Число  $n$  — длина регистра.
- Отображение  $f$  — функция обратной связи.
- Переменные  $x_1, \dots, x_n$  — внутренние переменные.
- Переменная  $x_{n+1}$  — входная переменная.

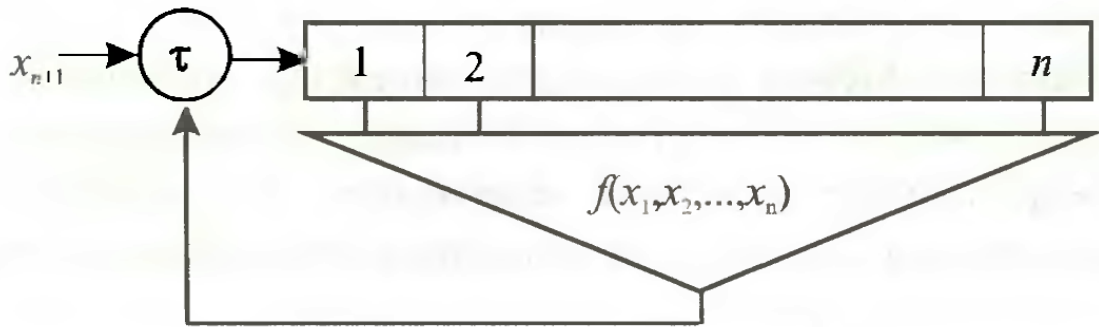


Рис. 1: Неавтономный регистр правого сдвига длины  $n$ .

Обычно  $X$  — кольцо или поле, а  $\tau$  биективна по обоим переменным и реализует сложение.

Отображение регистра сдвига над кольцом  $X$  является линейным, если линейна функция обратной связи. Соответствующие регистры называются **линейными регистрами сдвига (ЛРС)** над кольцом  $X$ .

**Теорема:** Преобразование  $fg$  автономного регистра левого сдвига множества  $X^n$  биективно  $\iff$  функция обратной связи  $f : X^n \rightarrow X$  биективна по переменной  $x_1$  (по выталкиваемой переменной).

**Следствие:** Преобразование  $fg$  регистра левого сдвига над  $GF(2)$  с обратной связью  $f : X^n \rightarrow X$  биективно  $\iff$   $f$  линейна по переменной  $x_1$ :

$$f(x_1, \dots, x_n) = x_1 \oplus \psi(x_2, \dots, x_n), \quad (10)$$

где  $\psi$  — произвольная б.ф. от  $n - 1$  переменной.

#### 4 Последовательность. Подпоследовательность, отрезок, мультиграмма. Функция перестановки, замены, сопряжения. Период и предпериод последовательности. Чисто периодическая последовательность. Утверждение о длинах предпериода и периода последовательности; об изменении длин периода и предпериода при замене членов последовательности.

Пусть  $X_{\rightarrow} = \{x_1, \dots, x_i, \dots\}$  - бесконечная последовательность на мн-вом  $X$  порядка  $k$ .

Последовательность  $\{x_{j_1}, x_{j_2}, \dots, x_{j_i}, \dots\}$  при  $1 \leq j_1 < j_2 < \dots < j_i < \dots$  называется подпоследовательностью пос-ти  $X_{\rightarrow}$ .

Подпоследовательность  $\{x_r, x_{r+1}, \dots, x_{r+s-1}\}$  называется  $s$ -граммой пос-ти  $X_{\rightarrow}$  (или  $[r, r+s-1]$ -отрезком  $X_{\rightarrow}$ ). При  $s > 1$  она называется мультиграммой.

Пос-ть  $X_{\rightarrow}$  называется периодической, если  $x_i = x_{i+\tau}$  при  $i > \mu$ , где  $\tau \in \mathbb{N}, \mu \in \mathbb{N}_0$  (в  $X_{\rightarrow}$  имеются совпадения на расстоянии  $\tau$ , начиная с  $\mu + 1$ ). Наименьшее такое  $\tau$  называется длиной периода последовательности и обозначается через  $t(X_{\rightarrow})$ . Длиной предпериода пос-ти ( $\nu(X_{\rightarrow})$ ) называется наименьшее  $\nu \in \mathbb{N}_0$ , при котором имеются совпадения на расстоянии  $t(X_{\rightarrow})$ , начиная с номера  $\nu + 1$ .

Предпериодом называется  $[1, \nu]$ -отрезок, а периодом -  $[\nu + i, \nu + i + t - 1]$ -отрезок,  $i \in \mathbb{N}$ .

Чисто периодической последовательностью называется пос-ть  $X_{\rightarrow}$ , для которой  $\nu(X_{\rightarrow}) = 0$ .

**Утверждение:**

1. Если в  $X_{\rightarrow}$  имеются совпадения на расстоянии  $\tau$ , начиная с номера  $\mu + 1$ , то  $t \mid \tau$  и  $\nu = \mu$ .
2. Если пос-ть  $Y_{\rightarrow} = f^*(X_{\rightarrow}) = \{f(x_i)\}$ , где  $X_{\rightarrow} = \{x_i\}$  - периодическая, а  $f : X \rightarrow Y$ , то  $Y_{\rightarrow}$  - тоже периодическая, при этом:  $\nu(Y_{\rightarrow}) \leq \nu(X_{\rightarrow})$  и  $t(X_{\rightarrow}) \mid t(Y_{\rightarrow})$ . При этом если  $f$  - биекция, то  $\nu(Y_{\rightarrow}) = \nu(X_{\rightarrow})$  и  $t(X_{\rightarrow}) = t(Y_{\rightarrow})$ .

#### 5 Теорема о связи длин периода и предпериода последовательностей специального вида над конечной аддитивной группой (без доказательства). Утверждение о длинах предпериода и периода сопряжения последовательностей, следствие (без доказательства). Усложненная последовательность. Верхние и нижние оценки длины периода усложненной последовательности (без доказательства).

**Теорема:** Для пос-тей  $X_{\rightarrow}$  и  $Y_{\rightarrow}$  над конечной аддитивной группой  $X$ , где  $y_i = \sum_{j=1}^i x_j$ , выполнено:

1. Если  $X_{\rightarrow}$  - периодическая с длиной предпериода  $\nu > 0$  и длиной периода  $t$ , то  $Y_{\rightarrow}$  - периодическая с длиной предпериода  $\nu - 1$  и длиной периода  $t'$ , где  $t' \mid d \cdot t$ , где  $d$  - порядок эл-та  $y_{\nu+t} - y_{\nu}$  группы  $X$ .

2. Если  $X_{\rightarrow}$  - чисто периодическая с длиной периода  $t$ , то  $Y_{\rightarrow}$  - чисто периодическая с длиной периода  $t'$ , где  $t' \mid d \cdot t$ , где  $d$  - порядок эл-та  $y_t$  группы  $X$

**Утверждение:**

1.  $X_{\rightarrow}$  - пос-ть над  $X = X_1 \times \dots \times X_n$  периодическая  $\iff X_{\rightarrow}^{(j)}$  - периодическая  $j = \overline{1, n}$ . При этом верно:

$$\nu(X_{\rightarrow}) = \max\{\nu(X_{\rightarrow}^{(1)}), \dots, \nu(X_{\rightarrow}^{(n)})\} \quad (11)$$

$$t(X_{\rightarrow}) = [t(X_{\rightarrow}^{(1)}), \dots, t(X_{\rightarrow}^{(n)})] \quad (12)$$

2. Если пос-ть  $X_{\rightarrow}^{(j)}$  отличается от  $X_{\rightarrow}^{(1)}$  лишь сдвигом на  $j - 1$  знак, то верно:

$$\nu(X_{\rightarrow}) = \nu(X_{\rightarrow}^{(1)}) \quad (13)$$

$$t(X_{\rightarrow}) = t(X_{\rightarrow}^{(1)}) = \dots = t(X_{\rightarrow}^{(n)}) \quad (14)$$

**Следствие:** Если  $X_{\rightarrow}$  - периодическая последовательность над  $X = X_1 \times \dots \times X_n$  и  $t(X_{\rightarrow}) = p^m$ ,  $p$  - простое,  $m \in \mathbb{N}$ , то  $t(X_{\rightarrow}^{(j)}) = p^{m_j}$ ,  $j = \overline{1, n}$ , где  $0 \leq m_j \leq m$  и  $\max\{m_1, \dots, m_n\} = m$

Последовательность  $Y_{\rightarrow} = \{f(x_{i,1}, \dots, x_{i,n})\}, i \geq 0$ , полученную из пос-ти  $X_{\rightarrow} = \{x_{i,1}, \dots, x_{i,n}\}$  над  $X = X_1 \times \dots \times X_n$  с помощью ф-ции усложнения  $f : X \rightarrow Y$ , называются усложненной последовательностью по отношению к исходным пос-тям  $X_{\rightarrow}^{(j)}, j = \overline{1, n}$ .

Верхняя оценка периода  $Y_{\rightarrow}$ :

$$t_Y \mid [t_1, \dots, t_n] \quad (15)$$

Нижние оценки:

Если  $X_{1\rightarrow}$  и  $X_{2\rightarrow}$  - пос-ти над аддитивной группой  $X$  с периодами  $t_1, t_2$  соответственно, а  $f(x_1, x_2) = x_1 + x_2$ , то верно:

$$\frac{[t_1, t_2]}{(t_1, t_2)} \leq t_Y \quad (16)$$

Если  $f : X_1 \times \dots \times X_n \rightarrow Y$  биективна по переменным с номерами  $j_1, \dots, j_b$  ( $\{j_1, \dots, j_b\} \subseteq \{1, \dots, n\}$ ), то верна оценка:

$$t_Y \geq \prod_{l=1}^b \frac{\Theta}{\Theta_{j_l}} \quad (17)$$

где  $\Theta = [t_1, \dots, t_n]$ ,  $\Theta_j = [t_1, \dots, t_{j-1}, t_{j+1}, \dots, t_n]$ ,  $j = \overline{1, n}$

**Следствие:** Если  $f$  биективна по каждой переменной, а  $(t_1, \dots, t_n) = 1$ , то длина периода  $Y_{\rightarrow}$  максимальна:  $t_Y = t_1 \cdot \dots \cdot t_n$

**6 Период и предпериод элемента относительно преобразования, свойства. Утверждение о связи длин периода и предпериода элемента относительно преобразования с графом преобразования, замечание (без доказательства). Период и предпериод преобразования. Утверждение о связи длин периода и предпериода преобразования с графом преобразования, замечание (без доказательства).**

Пусть  $g \in \Pi(X)$ .  $g_{\rightarrow} = \{g^i\}, i = 1, 2, \dots$  - пос-ть над моноидом  $\Pi(X)$ ,  $g_{\rightarrow}(x) = \{g^i(x)\}$  - пос-ть над  $X$ .

Периодом (предпериодом) элемента  $x$  относительно преобразования  $g$  называется период (предпериод) пос-ти  $g_{\rightarrow}(x)$ . Их длины обозначаются через  $t_{x,g}, \nu_{x,g}$  или  $t_x, \nu_x$ .

**Утверждение:**  $\forall g \in \Pi(X), x \in X$ :

$$t_{x,g} + \nu_{x,g} \leq |X| \quad (18)$$

Если  $x$  - циклическая вершина графа  $\Gamma(g)$ , то  $\nu_{x,g} = 0$ ,  $t_{x,g}$  равна длине цикла, которому принадлежит вершина  $x$

Если  $x$  - ациклическая вершина графа  $\Gamma(g)$ , то  $\nu_{x,g}$  равна длине подхода из  $x$  к циклу  $C$ , а  $t_{x,g}$  - длина этого цикла

(Замечание ???)

Периодом (пердпериодом) преобразования  $g$  называется период (предпериод) пос-ти  $g_{\rightarrow}$  (обозначение:  $t_g, \nu_g$ )

**Утверждение:** величины  $t_g, \nu_g$  - период и циклическая глубина эл-та  $g$  моноида  $\Pi(X)$   $\forall g \in \Pi(X)$  :  $t_g = [l_1, \dots, l_n]$ ,  $l_1, \dots, l_n$  - длины циклов графа  $\Gamma(X)$ .

Если  $g$  - обратимое преобразование, то  $\nu_g = 0$ , иначе  $\nu_g$  - наибольшая из длин подходов в графе  $\Gamma(g)$

(Замечание ???)

## 7 Полноцикловое преобразование. Теорема о количестве различных полноцикловых преобразований. Линейный конгруэнтный генератор (ЛКГ). ЛКГ полного периода. Критерий максимальности длины периода ЛКГ (без доказательства). Критерий полноцикловости треугольного преобразования с координатными функциями специального вида (без доказательства).

Преобразование  $g \in \Pi(X)$  называется полноцикловым, если  $\Gamma(g)$  представляет из себя один цикл длины  $n$ , где  $n = |X|$ .

**Теорема:** Всего различных п.ц. преобразований ровно  $(n - 1)!$

Преобразование  $g \in \Pi(\mathbb{Z}_k)$  называется ЛКГ, если:

$$\forall x \in \mathbb{Z}_k : g(x) = (a \cdot x + b) \bmod k \quad (19)$$

где  $a, b, k$  - множитель, сдвиг и модуль соответственно.

Для любого  $k$  найдутся такие  $a, b$ , что ЛКГ будет преобразованием максимального периода. При этом длина периода не превышает  $k$ .

**Теорема:** Длина периода ЛКГ равна  $k \iff$  выполнены условия:

1.  $(b, k) = 1$
2.  $a - 1$  делит любой простой делитель  $k$
3.  $a - 1$  делит 4, если  $k$  делит 4

В частности:  $t_g = k$  при  $k = 2^r \iff b$  - нечетное и  $a \equiv 1 \pmod{4}$

Пусть  $g_i$  - треугольная подстановка мн-ва  $X^i$  задана системой координатный ф-ций:

$$g_i = \{f_1(x_1), \dots, f_i(x_1, \dots, x_i)\} \quad (20)$$

**Критерий:** Пусть  $f_i(x_1, \dots, x_i) = h(x_1, \dots, x_{i-1}) \oplus x_i, i = \overline{1, n}$ . Треугольная подстановка  $g_n$  мн-ва  $X^n$  является полноциклового  $\iff h_1 = 1, ||h_i||$  нечетен  $i = \overline{2, n}$

## 8 Принцип склеивания-расклеивания, основополагающая теорема. Линейные преобразования максимального периода. Сопровождающая матрица и характеристический многочлен линейного регистра сдвига (ЛРС). Критерий максимальной длины периода ЛРС (без доказательства). Свойства примитивных многочленов.

**Теорема** (принцип склеивания-расклеивания): Пусть  $g, h$  - подстановки двоичных регистров сдвига (автономных) длины  $n > 1$  и функциями обратной связи  $f(x_1, \dots, x_n)$  и  $f(x_1, \dots, x_n) \oplus x_2^{\alpha_2} \cdot \dots \cdot x_n^{\alpha_n}$  соответственно, где  $\alpha_2, \dots, \alpha_n \in \{0, 1\}$ . Тогда граф  $\Gamma(g)$  отличается от графа  $\Gamma(h)$  тем, что либо один цикл из  $\Gamma(g)$  распадается на два цикла в  $\Gamma(h)$ , либо два цикла в  $\Gamma(g)$  объединяются в один цикл в  $\Gamma(h)$

Линейное преобразование пространства  $P^n$ , где  $P$  - поле, не может быть полноцикловым, так как нулевой элемент поля является его неподвижной точкой. Однако длина цикла в графе преобразования может составлять  $k^n - 1$ , где  $k = |P|$ . Такие преобразования называют преобразованиями максимального периода.

Рассмотрим преобразование  $g$  ЛРС (линейного регистра сдвига) с ф-цией обратной связи  $a_{n-1}x^n + \dots + a_1x_2 + a_0x_1$ , где  $a_{n-1}, \dots, a_0 \in P$ . Сопровождающей матрицей данного преобразования называется матрица:

$$A_g = \begin{pmatrix} 0 & 0 & \dots & 0 & a_0 \\ 1 & 0 & \dots & 0 & a_1 \\ 0 & 1 & \dots & 0 & a_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & a_{n-1} \end{pmatrix} \quad (21)$$

Для реализации преобразования вектор  $(x_1, \dots, x_n)$  умножается на  $A_g$  слева. Характеристическим полиномом ЛРС называется полином:

$$F(\lambda) = \lambda^n - a_{n-1}\lambda^{n-1} - \dots - a_1\lambda - a_0 \quad (22)$$

$A_g$  является корнем  $F(\lambda)$ . Если  $F(\lambda)$  неприводим над  $P$ , то порядок матрицы совпадает с порядком полинома.

**Критерий:**  $g$  имеет максимальный период  $\iff F(\lambda)$  примитивен.

$F(\lambda)$  является неприводимым, если:

- $F(\lambda)$  неприводим над  $P$
- $F(\lambda)$  делит полином  $\lambda^{k^n-1} - 1$  и не делит ни один из следующих:  $\lambda^d - 1, d \mid k^n - 1 \wedge d \neq k^n - 1$

Для полиномов над  $GF(2)$  верны следующие свойства:

- Если  $F(\lambda)$  степени  $n > 1$  неприводим над  $GF(2)$ , а  $2^n - 1$  - простое число, то преобразование ЛРС мн-ва  $V_n$  имеет максимальный период
- Примитивный полином над  $GF(2)$  содержит нечетное число членов
- Если  $F(\lambda)$  примитивен над  $GF(2)$ , то примитивен над  $GF(2)$  и  $\lambda^n \cdot F(1/\lambda)$



- 9 Равномерно распределенные случайные последовательности, свойства. Псевдослучайные последовательности. Рекуррентные последовательности (РП), линейные рекуррентные последовательности (ЛРП). Замечание о длине периода РП. Замечание о связи множества РП и множества регистров сдвига. Замечание о связи множества ЛРП и множества ЛРС.
- 10 ЛРП максимального периода. Характеристический многочлен ЛРП. Утверждение о количестве мультиграмм на периоде ЛРП максимального периода. Замечание о низкой стойкости ЛРП. Аннулирующий и минимальный многочлены последовательности, свойства (без доказательства). Линейная сложность последовательности. Профиль линейной сложности последовательности.
- 11 Утверждения о минимальном многочлене сопряжения и линейной комбинации последовательностей. Замечания о линейной сложности суммы и почленного произведения последовательностей (без доказательства). Нормальная рекуррентная последовательность. Компенсированная последовательность. Теорема о минимальном многочлене чисто периодической последовательности (без доказательства), следствие. Замечание о линейной сложности НРП  $(2, n)$  (без доказательства).
- 12 Поточные шифры. Синхронные поточные шифры (СПШ). Устройство СПШ. Общая и базовая схемы СПШ. Классификация СПШ по способу построения генератора гаммы. Свойства СПШ. Атака вставкой. Необходимые условия криптографически стойкого СПШ, требования к управляющей гамме. Слабый ключ СПШ.
- 13 Самосинхронизирующиеся поточные шифры (ССПШ). Сходства и отличия СПШ и ССПШ. Общая схема ССПШ. Атака повторной передачи, способы защиты. Свойства