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, следствия.

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

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

Теорема:

$$\varphi : X^n \to X^m \iff F_{m,n} = \{f_1(x_1, ..., x_n), ..., f_m(x_1, ..., x_n)\} \tag{2}$$

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

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

Весовые характеристики:

$$N^{i_1,...,i_s}_{r_1,...,r_s} = |\{(x_1, ..., x_n) \in X^n \mid f_{i_1}(x_1, ..., x_n) = r_1, ..., f_{i_s}(x_1, ..., x_n) = r_s\}| \tag{3}$$

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

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

$$N^{i_1,...,i_s}_{r_1,...,r_s} = k^{n-s} \tag{4}$$

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 $\{i_1, ..., i_s\}$ мн-ва $\{1, ..., m\}$:

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

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 $\exists \psi : X^m \to X$, отличная от константы, для которых

$$\psi(f_1(x_1, ..., x_n), ..., f_m(x_1, ..., x_n)) \equiv b \tag{6}$$

Теорема: Отображение φ, определяемое системой $F_{m,n}$, сюрьективно $\iff$ $F_{m,n}$ - АНЗ
Следствие: Преобразование g множества X^n биективно $\iff$ АНЗ система его координатных ф-ций.

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

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

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

$$\varphi(x) = \psi(x) + a \tag{8}$$

где ψ - линейная функция, $a \in P^m$
Ф-ция, отличная от аффинной, назвывается нелинейной.

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

3 Треугольное преобразование декартовой степени конечного 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 $g_n = F_{\Delta,n} = \{f_1(x_1), f_2(x_1, x_2), ..., f_n(x_1, ..., x_n)\}$, иначе если $S(f_i) \subseteq 1, ..., i$ для $i = 1, ..., n$, где $S(f)$ — множество номеров существенных переменных функции f.
Теорема: Треугольное преобразование g_n множества X^n биективно $\iff$ функция $f_i(x_1, ..., x_i)$ биективна по последней переменной x_i, $i = 1, ..., n$.

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

$$ {}_f\varphi(x_1, ..., x_n, x_{n+1}) = (x_2, ..., x_n, \tau\left(f(x_1, ..., x_n), x_{n+1}\right)). \tag{9}$$

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

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

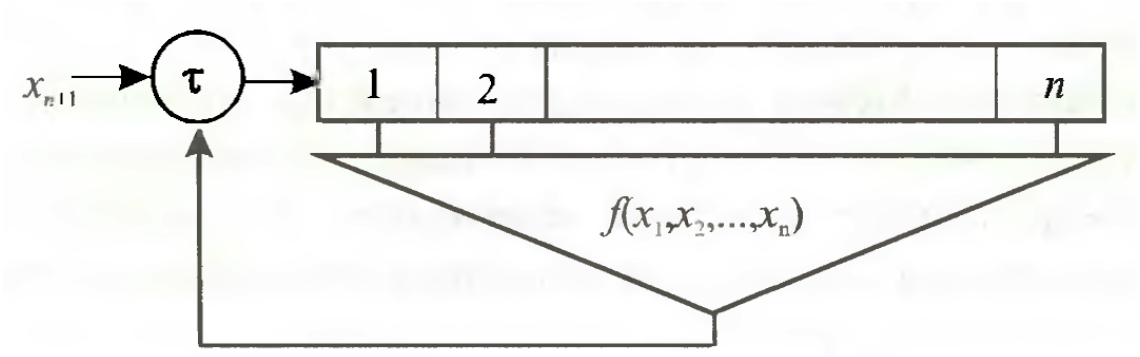


Рис. 1: Неавтономный регистр правого сдвига длины n.

Обычно X — кольцо или поле, а τ биективна по обеим 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 $f : X^n \to X$ биективна по переменной x_1 (по выталкиваемой переменной).

Следствие: Преобразование ${}_fg$ регистра левого сдвига над $GF(2)$ с обратной связью $f : X^n \to X$ биективно $\iff$ f линейна по переменной x_1:

$$ f(x_1, ..., x_n) = x_1 \oplus \psi(x_2, ..., x_n), \tag{10}$$

где ψ — 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 $X_\to = \{x_1, ..., x_i, ...\}$ - бусконечная последовательность на мн-вом X порядка k.

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

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

Пос-ть $X_\to$ называется периодической, если $x_i = x_{i+\tau}$ при $i > \mu$, где $\tau \in \mathbb{N}, \mu \in \mathbb{N}_0$ (в $X_\to$ имеются совпадения на расстоянии τ, начиная с $\mu + 1$). Наименьшее такое τ называется длиной периода последовательности и обозначается через $t(X_\to)$. Длиной предпериода пос-ти ($\nu(X_\to)$) называется наименьшее $\nu \in \mathbb{N}_0$, при котором имеются совпадения на расстоянии $t(X_\to)$, 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 $X_\to$, для которой $\nu(X_\to) = 0$

Утверждение:

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

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 $X_\to$ и $Y_\to$ над конечной аддитивной группой X, где $y_i = \sum_{j=1}^{i} x_j$, выполнено:

1. Если $X_\to$ - периодическая с длиной предпериода $\nu > 0$ и длиной периода t, то $Y_\to$ - 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 $X = X_1 \times ... \times X_n$ периодическая $\iff$ $X_\rightarrow^{(j)}$ - периодическая $j = \overline{1,n}$. При этом верно:
$$\nu(X_\rightarrow) = \max\{\nu(X_\rightarrow^{(1)}), ..., \nu(X_\rightarrow^{(n)})\} \tag{11}$$
$$t(X_\rightarrow) = [t(X_\rightarrow^{(1)}), ..., t(X_\rightarrow^{(n)})] \tag{12}$$
2. Если пос-ть $X_\rightarrow^{(j)}$ отличается от $X_\rightarrow^{(1)}$ лишь сдвигом на $j-1$ знак, то верно:
$$\nu(X_\rightarrow) = \nu(X_\rightarrow^{(1)}) \tag{13}$$
$$t(X_\rightarrow) = t(X_\rightarrow^{(1)}) = ... = t(X_\rightarrow^{(n)}) \tag{14}$$

Следствие: Если $X_\rightarrow$ - периодическая последовательсность над $X = X_1 \times ... \times X_n$ 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 $0 \le m_j \le m$ и $\max\{m_1, ..., m_n\} = m$

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

Верхняя оценка периода $Y_\rightarrow$:
$$t_Y \mid [t_1, ..., t_n] \tag{15}$$

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:
$$\frac{[t_1, t_2]}{(t_1, t_2)} \le t_Y \tag{16}$$

Если $f : X_1 \times ... \times X_n \to Y$ биективна по переменным с номерами $j_1, ..., j_b$ ($\{j_1, ..., j_b\} \subseteq \{1, ..., n\}$), то верна оценка:
$$t_Y \ge \prod_{l=1}^{b} \frac{\Theta}{\Theta_{j_l}} \tag{17}$$
где $\Theta = [t_1, ..., t_n], \Theta_j = [t_1, ..., t_{j-1}, t_{j+1}, ..., t_n], j = \overline{1,n}$

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

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

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

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

$$t_{x,g} + \nu_{x,g} \leq |X| \tag{18}$$

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 $g_{\to}$ (обозначение: t_g, ν_g)

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

Если g - обратимое преобразование, то $\nu_g = 0$, иначе ν_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:

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

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:

$$g_i = \{f_1(x_1), ..., f_i(x_1, ..., x_i)\} \tag{20}$$

Критерий: Пусть $f_i(x_1, ..., x_i) = h(x_1, ..., x_{i-1}) \oplus x_i, i = \overline{1, n}$. Треугольная подстановка g_n мн-ва X^n является полноцикловой $\iff h_1 = 1, ||h_i||$ 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 максимальности 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 $f(x_1, ..., x_n)$ и $f(x_1, ..., x_n) \oplus x_2^{\alpha_2} \cdot ... \cdot x_n^{\alpha_n}$ соответственно, где $\alpha_2, ..., \alpha_n \in \{0, 1\}$. 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 (линейнго регистра сдвига) с ф-цией обратной связи $a_{n-1}x^n + ... + a_1x_2 + a_0x_1$, где $a_{n-1}, ..., a_0 \in P$. Сопровождающей матрицей данного преобразования называется матрица:

$$A_g = \begin{pmatrix} 0 & 0 & ... & 0 & a_0 \\ 1 & 0 & ... & 0 & a_1 \\ 0 & 1 & ... & 0 & a_2 \\ ... & ... & ... & ... & ... \\ 0 & 0 & ... & 1 & a_{n-1} \end{pmatrix} \tag{21}$$

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

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

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.

Случайная идеальная последовательность является реализацией последовательности независимых равномерно распределенных случайных величин. Такие последовательности называются РРСП (равномерно распределенными случайными пос-тями).

РРСП (на мн-ве X мощности k) - пос-ть $\{\zeta_1, ..., \zeta_t, ...\}$ случайных величин, принимающих значения на мн-ве X. Два требования к такой последовательности:

1. $\forall n\ \forall t_1, ..., t_n : 1 \leq t_1 < ... < t_n$ случайные величины $\zeta_{t_1}, ..., \zeta_{t_n}$ независимы в совокупности
2. $\forall t \in \mathbb{N}$ случайная величина ζ_t равномерно распределена на X

При выполнении требований справедливы свойства:

1. $\forall n\ \forall t_1, ..., t_n : 1 \leq t_1 < ... < t_n$ случайный вектор $(\zeta_{t_1}, ..., \zeta_{t_n})$ равномерно распределена на X^n
2. Воспроизводимость при прореживании: для $1 \leq t_1 < ... < t_n < ...$ соответствующая подпоследовательность $\zeta_{t_1}, ..., \zeta_{t_n}, ...$ также является РРСП
3. Воспроизводимость при суммировании: если X - аддитивная группа, а $\{\eta_t\}$ - произвольная неслучайная или произвольная случайная пос-ть над X, не зависящая от $\{\zeta_t\}$, то пос-ть $\{\zeta_t + \eta_t\}$ является РРСП.
4. $\forall t \in \mathbb{N}$ предсказание значения ζ_t по $\zeta_1, ..., \zeta_{t-1}$ невозможно, т.е. $Pr[\zeta_t = x_t \mid \zeta_1 = x_1, ..., \zeta_{t-1} = x_{t-1}] = Pr[\zeta_t = x_t] = 1/k$ для любого набора $(x_1, ..., x_t)$

Псевдослучайная последовательность (ПСП) имитирует РРСП, генерируется программным генератором (техническим устройством или программой).

Пос-ть $X_{\rightarrow}$ называется рекуррентной пос-тью (РП) порядка $n > 0$, если $\exists f : X^n \to X$

$$x_{i+n} = f(x_i, ..., x_{i+n-1}) \tag{23}$$

Равенство (23) называется законом рекурсии, f - генератором РП, а $(x_0, ..., x_{n-1})$ - начальным вектором РП. При $|X| = k$ РП порядка n обозначается как РП(k, n) Длина периода РП не превышает k^n.

Между мн-вом РП(k, n) и мн-вом регистров сдвига длины n над X существует биекция. Если генератор РП(k, n) совпадает с ф-цией обратной связи регистра сдвига, то РП(k, n) с начальным вектором $(x_0, ..., x_{n-1})$ есть первая координатная подпос-ть $X_{1\rightarrow}$ пос-ти ${}_f g(x_0, ..., x_{n-1})$, где ${}_f g$ является преобразованием X^n, реализуемое регистром

РП(k, n) над полем P называется линейной рекуррентной пос-тью (ЛРП(k, n)), если для некоторых констант $a_0, ..., a_{n-1}$ (не всех нулей) верно:

$$x_{i+n} = \sum_{j=0}^{n-1} a_j \cdot x_{i+j} \tag{24}$$

Характеристический полином ЛРП(k, n):

$$F(\lambda) = \lambda^n - a_{n-1}\lambda^{n-1} - ... - a_1\lambda - a_0 \tag{25}$$

Между мн-вом ЛРП(k, n) и мн-вом ЛРС длины n над P существует биекция. Если характеристические полиномы ЛРП(k, n) и ЛРС совпадают и равны $F(\lambda)$, то ЛРП(k, n) есть первая координатная подпос-ть пос-ти ${}_f g(x_0, ..., x_{n-1})$, где при $a_0 \neq 0$ ${}_f g$ является линейной подстановкой на P^n, реализуемая ЛРС с ф-цией обратной связи f, соответствующей характеристическому полиному $F(\lambda)$

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.

ЛРП максимального периода порождается от ненулевого начального вектора тогда и только тогда, когда ее характеристический полином примитивен

Утверждение: на периоде ЛРП длины n максимального периода над полем P порядка k всякая ненулевая s-грамма встречается k^{n-s} раз, а нулевая s-грамма встречается $k^{n-s} - 1$ раз $(1 \leq s \leq n)$

Замечание: В ЛРП(k, n) имеется простая межнаковая зависимость, позволяющая по любой n-грамме ЛРП(k, n) определить начальный вектор, решив СЛАУ.

Пусть $X_\rightarrow$ - пос-ть над P^m - векторны пространством над полем P. Ненулевой полином $F(\lambda)$ называется аннулирующим полиномом пос-ти $X_\rightarrow$, если:

$$\forall j \geq n : x_j - a_{n-1}x_{j-1} - ... - a_1 x_{j-n+1} - a_0 x_{j-n} = u \tag{26}$$

где u - нулевой элемент P^m

Минимальным полиномом ($m_{X_\rightarrow}(\lambda)$) называется аннулирующий полином наименьшей степени.
Свойства:

1. Если $f(\lambda) \in Ann(X_\rightarrow)$, то $f(\lambda) \cdot g(\lambda) \in Ann(X_\rightarrow)$ для любого ненулевого полинома $g(\lambda)$
2. Если $f_1(\lambda), ..., f_r(\lambda) \in Ann(X_\rightarrow)$, то любая нетривиальная линейная комбинация этих полиномов над P также является аннулирующим полиномом
3. $m_{X_\rightarrow}(\lambda)$ определен однозначно и делит любой аннулирующий полином
4. Чисто периодическая пос-ть $X_\rightarrow$ с длиной периода t аннулируется полиномом $\lambda^t - 1$ и $m_{X_\rightarrow}(\lambda) \mid \lambda^t - 1$

Линейная сложность пос-ти $X_\rightarrow$:

$$\Lambda(X_\rightarrow) = \deg\, m_{X_\rightarrow}(\lambda) \tag{27}$$

Еще линейную сложность можно определить как порядок самой короткой ЛРП, способной породить $X_\rightarrow$ при некотором начальном векторе $(x_1, ..., x_{n-1})$

Профиль линейной сложности - последовательность $\{\Lambda_t\}$, где Λ_t - линейная сложность отрезка $\{x_0, ..., x_t\}$. Известно, что для случайной идеальной пос-ти: $E[\Lambda_t] \sim t/2$, $D[\Lambda_t]$ ограничена константой, убывающей с ростом порядка поля.

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).

Утверждение: Пусть $X_\rightarrow = X_{1\rightarrow} \circ ... \circ X_{n\rightarrow}$, тогда:

$$m_{X_\rightarrow}(\lambda) = [m_1(\lambda), ..., m_n(\lambda)] \tag{28}$$

где $m_j(\lambda)$ - минимальный полином пос-ти $X_{j\rightarrow}$

Утверждение: Пусть $X_{\rightarrow} = a_1 \cdot X_{1\rightarrow} + ... + a_n \cdot X_{n\rightarrow}$ ($a_j \in P, i\overline{1,n}, P$ - поле), тогда:

$$m_{X_{\rightarrow}}(\lambda) \mid [m_1(\lambda), ..., m_n(\lambda)] \tag{29}$$

Замечание: Нижняя граница линейной сложности суммы $X_{\rightarrow}$ пос-тей $X_{1\rightarrow}, X_{2\rightarrow}$:

$$\deg m_{X_{\rightarrow}}(\lambda) \geq \deg m_1(\lambda) + \deg m_2(\lambda) - 2(t_1, t_2) \tag{30}$$

где t_1, t_2 - периоды $X_{1\rightarrow}, X_{2\rightarrow}$ соответственно. В частности, когда $(t_1, t_2) = 1$ и $\lambda - 1 \mid m_1(\lambda) \cdot m_2(\lambda)$: $\Lambda(X_{\rightarrow}) = \Lambda(X_{1\rightarrow}) + \Lambda(X_{2\rightarrow})$

Замечание: Верхняя граница линейной сложности произведения $X_{\rightarrow}$ пос-тей $X_{j\rightarrow}, j = \overline{1,n}$:

$$\Lambda(X_{\rightarrow}) = \prod_{j=1}^{n} \Lambda(X_{j\rightarrow}) \tag{31}$$

Граница достигается при условии, что поле P имеет простой порядок, а $m_j(\lambda)$ примитивны над ним и имеют попарно взаимнопростые степени

Чисто перриодическую РП(k, n) над мн-вом X называют нормальной рекуррентной пос-тью (НРП(k, n)), если длина ее периода равна k^n. Генератором НРП(k, n) является ф-ция $f : X^n \to X$, реализующая обратную связь полноциклового регистра сдвига длины n. При этом для регистра левого сдвига f биективна по первой переменной.

НРП(k, n) над полем P может быть получена из ЛРП максимального периода вставкой нуля в цикл. Каждая s-грамма тогда будет на цикле встречаться ровно k^{n-s} раз. Линейная сложность НРП выше, чем у ЛРП.

Пос-ть $X_{\rightarrow}$ над P^m называется компенсированной, если при длине периода, равной t, верно:

$$x_1 + ... + x_n = u \tag{32}$$

где u - нулевой элемент P^m

Теорема: Пусть $X_{\rightarrow}$ - чисто периодическая последовательность над P^m с длиной периода k^r. Тогда:

$$m_{X_{\rightarrow}}(\lambda) = (\lambda - 1)^s \tag{33}$$

где $k^{r-1} < s < k^r - \zeta(X_{\rightarrow})$, и

$$\zeta(X_{\rightarrow}) = \begin{cases} 0 & \text{если } X_{\rightarrow} \text{ не компенсированная} \\ 1 & \text{иначе} \end{cases} \tag{34}$$

при этом $s = k^{r-1} + 1$, если $x_{i+k^{r-1}} - x_i \neq u, i = \overline{1, k^r}$

Замечание: для НРП$(2, n)$ $X_{\rightarrow}$ при $n \geq 3$:

$$2^{n-1} + n \leq \Lambda(X_{\rightarrow}) \tag{35}$$

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.

Поточный шифр - шифр замены, преобразующий открытый текст в шифртекст посимвольно. Поточный шифр преобразуется символ открытого текста x_i в символ шифртекста y_i путем применения меняющихся от такта к такту шифрующих отображений $\varphi_i : X \to Y$

СПШ состоит из управляющего блока, который генерирует гамму, и шифрующего блока, который накладывает гамму на открытый текст или шифртекст при зашифровании и расшифровании соответственно (рис. 2).

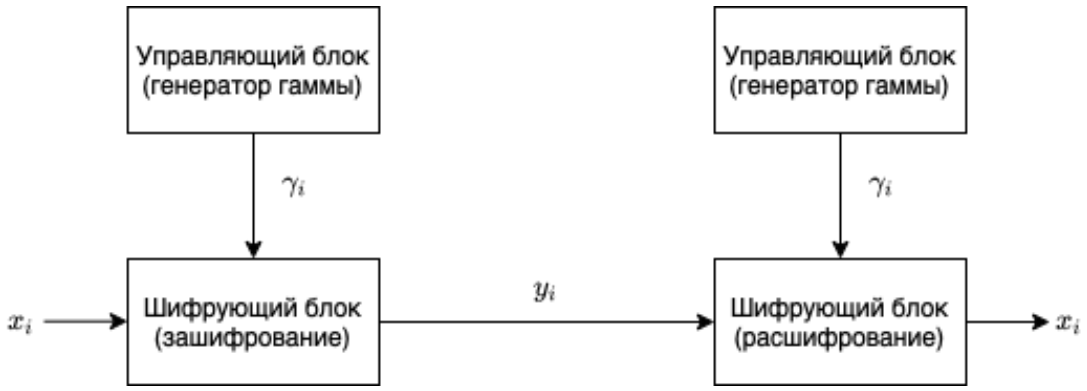


Рис. 2: Схема СПШ.

СПШ делятся по способо построения УБ на два класса:

1. С генератором типа счетчика. В таких генераторах от ключа зависит только функция выхода
2. С генератором с внутренней обратной связью. В таких генераторах от ключа зависит внутренняя функция переходов или начальное заполнение генератора. При этом функция выхода от ключа не зависит

Свойства СПШ:

1. Может возникнуть рассинхронизация. Способы борьбы: перешифровать сообщение на заново инициализированном ключе или разбить сообщения на блоки, вставляя после каждого блока специальные маркеры
2. Ошибки не распространяются, так как генератор гаммы автономен
3. "Защита" от несанкционированных вставок и удалений. Рассинхронизация будет замечена (возможно)
4. Отсутствует защита от подмены отрезка сообщения на отрезок той же длины
5. Уязвимость к атаке вставкой

Атака вставкой:

1. Перехват криптограммы:

$$\begin{array}{cccc} x_1 & x_2 & x_3 & \dots \\ \downarrow & \downarrow & \downarrow & \dots \\ \gamma_1 & \gamma_2 & \gamma_3 & \dots \\ \hline y_1 & y_2 & y_3 & \dots \end{array}$$

2. Вставка:

$$\begin{array}{cccc} x_1 & \alpha & x_2 & \dots \\ y_1 & \dots & \dots & \dots \end{array} \leftarrow \text{рассинхронизация}$$

   α является известным значением, а его местоположение определяется просто

3. Решение системы:

$$\gamma_2 = \alpha \oplus y'_2 \qquad \gamma_3 = x_2 \oplus y'_3$$
$$x_2 = \gamma_2 \oplus y_2 \qquad x_3 = \gamma_3 \oplus y_3$$

Совершенно стойкий шифр - шифр, для которого шифртекст и открытый текст статистически независимы.

Идеально стойкий шифр - шифр, для которого невозможно однозначно определить открытый текст по известному шифртексту сколь угодно большой длины.

Необходимые условия криптографически стойкого СПШ следуют из того, что наилучшей имитацией идеального шифра является шифр, в котором пос-ть шифрующих отображений имитирует пос-ть независимых случайных отображений. Сами условия:

1. При каждом фиксированном $x \in X$ отображение $f(\gamma, x)$ является сбалансированным (как следствие: $|Y| \mid |\Gamma|, |X| \mid |\Gamma|$

2. При случайном равновероятном выборе ключа управляющая гамма наиболее хорошо имитирует идеальную случайную пос-ть (РРСП на Г)

Из второго условия вытекают требования к гамме:

1. Гамма должна иметь большую длину периода и не содержать длинных повторяющихся отрезков

2. Гамма должна быть равновероятной

3. Восстановление гаммы по ее отрезку должно быть трудной задачей. В частности нужна высокая линейная сложность.

4. Система уравнений гаммобразования должна иметь высокую сложность решения

Слабый ключ СПШ - ключ, при котором гамма не удовлетворяет хоятя бы одному из условий 1-3

13 Самосинхронизирующиеся поточные шифры (ССПШ). Сходства и отличия СПШ и ССПШ. Общая схема ССПШ. Атака повторной передачи, способы защиты. Свойства ССПШ. Шифры гаммирования. Групповые шифры гаммирования, шифры модульного гаммирования. Схема алгоритма поточного шифрования A5/1.

ССПШ отличается от СПШ строением УБ и схемой взаимодействия блоков. Схема изображена на рис. 3.

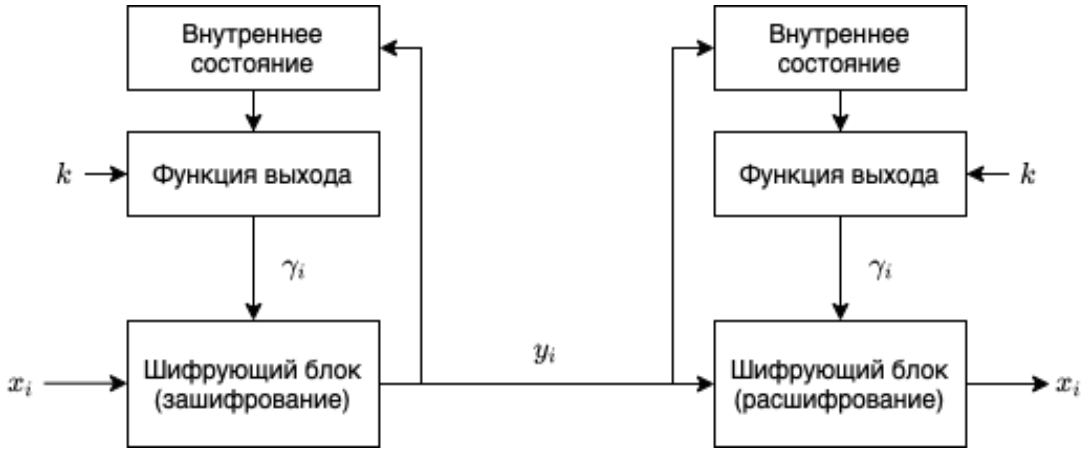


Рис. 3: Схема ССПШ.

Сходства с СПШ:

1. Наличие УБ и ШБ
2. Одинаковые уравнения зашифрования и расшифрования

Отличия от СПШ:

1. Внутреннее состояние ССПШ - n предшествующих битов шифртекста
2. От ключа в ССПШ зависит только функция выхода

Свойства ССПШ:

1. Самосихронизируется за n тактов. В случае потери бита будет расшифровано некорректно не более n бит
2. Распространение ошибок при искажении бита шифртекста, так как ошибка попадает в регистр сдвига
3. Уязвимость к атаке повторной передачи: если один и тот же отрезок текста перехватить и повторно отправить, то после восстановления синхронизма расшифрование снова будет корректным, а пользователь не сможет понять, что отправленный текст уже старый. Защититься можно, ставя метки времени или меняя ключ для кадого сообщения

Шифр гаммирования - поточный подстановочный шифр, в котором $X = Y$, а табличное задание шифрующего отображения дает латинский квадрат. Если мн-во $\Phi = \{\varphi_\gamma \mid \gamma \in \Gamma\}$ является группой, то такой шифр гаммирования называется групповым.

Если $X = Y = \Gamma = \mathbb{Z}_m$, а операция шифрования имеет вид

$$f(\gamma, x) = (\pm x \pm \gamma) \bmod m \tag{36}$$

то такой шифр называется шифром модульного гаммирования.

Шифр модульного гаммирования инволютивен, если:

$$y_i = x_i \oplus \gamma_i \tag{37}$$

$$y_i = (\pm\gamma_i - x_i) \bmod m \tag{38}$$

На рисунке 4 изображена схема генератора гаммы шифра A5/1, состоящая из 3 регистров сдвига. БУД отвечает за сдвиг регистров: сдвигаются регистры, тактирующие биты которых совпадают

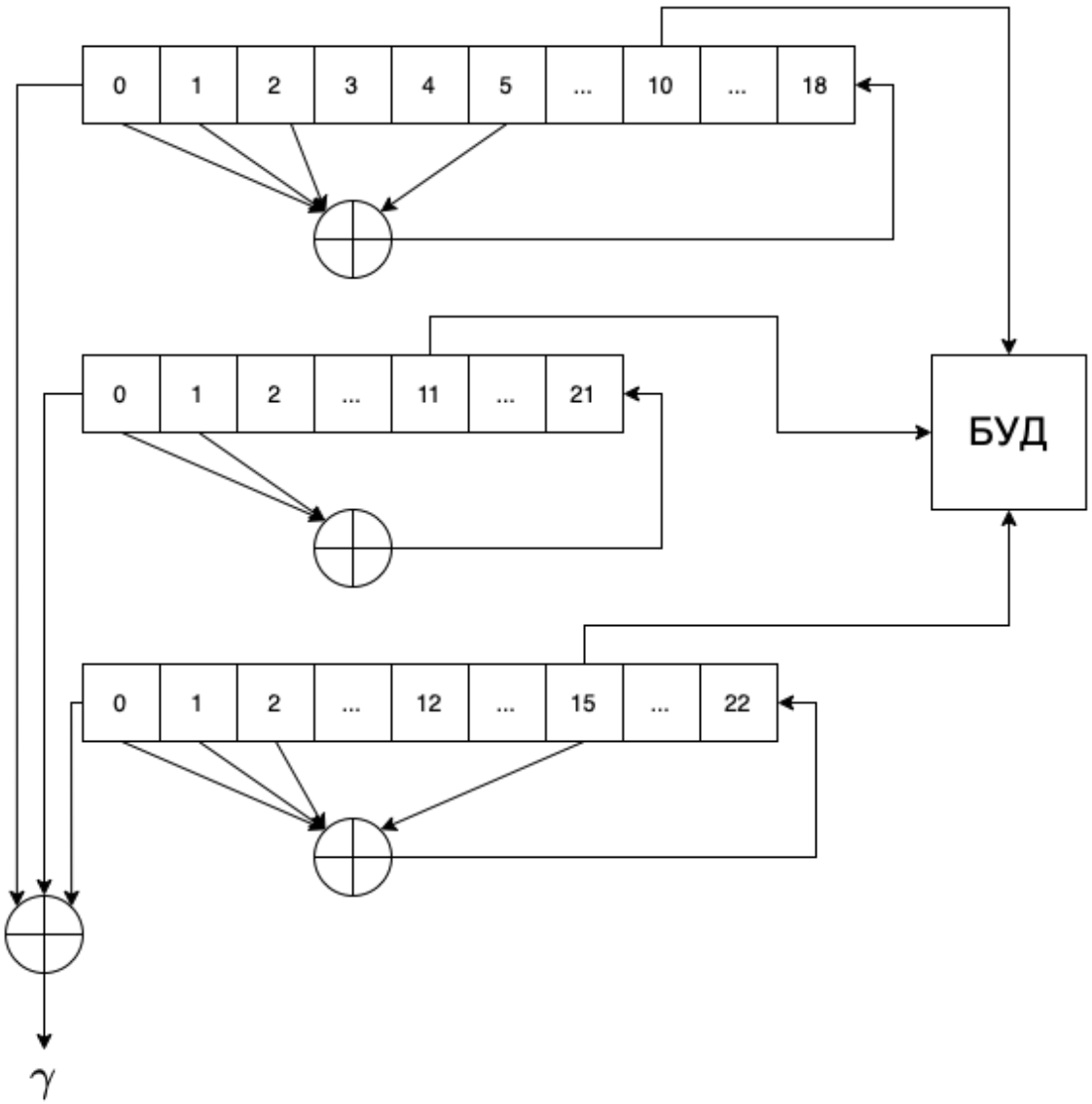


Рис. 4: Схема генератора гаммы для A5/1.

14 Симметричные блочные шифры (СБШ). Уравнения зашифрования в режиме простой замены. Принципы построения подстановки итеративного СБШ. Раундовые ключи, раундовые функции, входное и выходное отображения, ключевое расписание. Теорема об обратимости итеративного СБШ. Замечание об «отбеливании».

Симметричный блочный шифр шифрует информацию блоками. В режиме простой замен уравнение зашифрования выглядит следующим образом:

$$y_i = f(x_i, k) = E_k(x_i) \tag{39}$$

где $E_k(\cdot)$ - подстановка на множестве V_{2n}. Т.о. СБШ в режиме ECB реализует простую замену алфавита порядка 2^{2n}.

Пусть $\varphi : V_{2n} \times Q \to V_{2n}, \delta : V_{2n} \times Q' \to V_{2n}, \pi : V_{2n} \times Q' \to V_{2n}$ - биективные по первой переменной отображения. Для реализации подстановки E_k используются ключи:

$$\theta_i \in Q, i = \overline{1, r},\ \theta_j \in Q', j \in \{0, r+1\} \tag{40}$$

Подстановка E_k ИСБШ строится следующим образом:

$$E_k = \pi_{q_{r+1}} \cdot \varphi_{q_r} \cdot ... \cdot \varphi_{q_1} \cdot \delta_{q_0} \tag{41}$$

Выполнение подстановки φ_{q_i} называется i-м раундом шифрования, q_i - i-м раундовым ключом. $\delta_{q_0}, \pi_{q_{r+1}}$ - входным и выходным преобразованиями соответственно.

Система функций $\theta_i, i = \overline{0, r+1}$, с помощью которой из ключа получаются раундовые ключи, называется ключевым расписанием СБШ.

Теорема: Если $\forall q \in Q' : \delta_q = \pi_q^{-1}$, а $\forall q \in Q$ подстановка φ_q является инволюцией, то алгоритм шифрования ИСБШ обратим, и расшифрование отличается от зашифрования только применением раундовых ключей в обратном порядке.

Доказательство:

$$E_k^{-1} = \delta_{q_0}^{-1} \cdot \varphi_{q_1}^{-1} \cdot ... \cdot \varphi_{q_r}^{-1} \cdot \pi_{q_{r+1}}^{-1} \tag{42}$$

По утверждению теоремы: $\forall q \in Q' : \delta_q = \pi_q^{-1}$, а $\forall q \in Q$ подстановка φ_q является инволюцией, т.е.: $\forall q \in Q : \varphi_q^{-1} = \varphi_q$:

$$E_k^{-1} = \pi_{q_0} \cdot \varphi_{q_1} \cdot ... \cdot \varphi_{q_r} \cdot \delta_{q_{r+1}} \tag{43}$$

Теорема доказана.

Замечание: Если $Q' = V_{2n}$, а $\delta_{q_{r+1}}(x) = x \oplus q_{r+1}, \pi_{q_0}(y) = y \oplus q_0$, то применение $\delta_{q_0}, \pi_{q_{r+1}}$ называется отбеливанием текста, а q_0, q_{r+1} - ключами отбеливания

15 Шифры Фейстеля, схема реализации цикловой функции. Замечание об отличии шифров Фейстеля. Замечание о биективности шифра Фейстеля. Теорема об инволютивности шифра Фейстеля, вспомогательная лемма.

Шифр Фейстеля - ИСБШ, в котором раундовая функция выглядит следующим образом:

$$\varphi_{q_i}((x_1, x_2)) = (x_2, \psi(x_2, q_i) \oplus x_1) \tag{44}$$

где $x = (x_1, x_2), x_1, x_2 \in V_n$, ψ - функция усложнения.

Замечание: Фактически получается, что это преобразование автономного левого регистра сдвига с функцией обратной связи $\psi(x_2, q_i) \oplus x_1$. Биективность данного преобразования равносильна биективности функции обратной связи по x_1, что верно при любом ключе q_i и любой функции усложнения.

Замечание: Два шифра Фейстеля могут отличаться:

1. Функцией усложнения
2. Размером блока
3. Количеством раундов
4. Ключевым расписанием
5. Входным и выходным отображениями

Пусть $\langle T \rangle$ - группа циклических сдвигов в V_{2n}, ясно, что T^n - инволюция.
Лемма: При любой функции усложнения:

$$\varphi_q^{-1} = T^n \cdot \varphi_q \cdot T^n \tag{45}$$

Доказательство: простой подстановкой несложно показать, что $\varphi_q \cdot T^n \cdot \varphi_q \cdot T^n = e$. Лемма доказана.

Теорема: Если $\forall q \in Q' : \pi_q = \delta_q^{-1} \cdot T^n$, то алгоритм шифрования Фейстеля обратим и расшифрование отличается от зашифрования применением раундовых ключей в обратном порядке.
Доказательство: алгоритм зашифрования:

$$E_k = \pi_{q_{r+1}} \cdot \varphi_{q_r} \cdot ... \cdot \varphi_{q_1} \cdot \delta_{q_0} \tag{46}$$

Алгоритм расшифрования:

$$E_k^{-1} = \delta_{q_0}^{-1} \cdot \varphi_{q_1}^{-1} \cdot ... \cdot \varphi_{q_r}^{-1} \cdot \pi_{q_{r+1}}^{-1} \tag{47}$$

Применяя лемму выше и то, что T^n - инволюция, получаем:

$$E_k^{-1} = \delta_{q_0}^{-1} \cdot \varphi_{q_1}^{-1} \cdot ... \cdot \varphi_{q_r}^{-1} \cdot T^n \cdot \delta_{q_{r+1}} = \delta_{q_0}^{-1} \cdot T^n \cdot \varphi_{q_1} \cdot ... \cdot \varphi_{q_r} \cdot \delta_{q_{r+1}} \tag{48}$$

Теорема доказана.

16 Построение раундовой функции СБШ. Функциональное назначение конструктивных слоев цикловой функции СБШ. Условия, которым должна удовлетворять раундовая функция, s-боксы. Алгоритмы блочного шифрования DES, ГОСТ 28147-89: схема работы, ключевое расписание, основные количественные характеристики.

Будем полагать, что $Q = V_m \implies$ раундовая функция $\varphi_q : V_{2n+m} \to V_{2n}$, функция усложнения $\psi : V_{n+m} \to V_n$. Раундовая функция должна удовлетворять некотрым характеристикам, которые достигаются за счет того, что данная функция реализуется в виде "слоев каждый из которых обеспечивает некоторые из свойств.

Функциональное назнваение конструктивных слоев:

1. подмешивание производных (раундовых) ключей
2. перемешивание эл-тов входных блоков
3. реализация сложной нелинейной зависимости между знаками ключа, входного и выходного блоков

Раундовая функция должна удовлетворять следующим требованиям:

1. Для любого ключа она должна быть подстановкой, так как это требование вытекает из требования обратимости самой функции зашифрования $\implies$ должна быть сбалансированной. Стоит отметить, что функция усложнения шифра Фейстеля сбалансированной быть не обязана, но предпочтительнее использовать именно сбалансированной функции, так показали неоднократные исследования по криптоанализу.
2. Из соотношения ниже следует то, что при аффинности отображений $\varphi_q, \pi_1, \delta_q$ аффинна и вся функция E_k
$$E_k = \pi_{q_{r+1}} \cdot \varphi_{q_r} \cdot ... \cdot \varphi_{q_0} \cdot \delta_{q_0} \tag{49}$$
При этом ключ по шифртексту и открытому тексту определяется решением СЛАУ. А значит φ_q должна быть нелинейной, а ее координатные функции не должны допускать хороших аффинных приближений. При больших n задача упрощается, если нелинейный слой реализовать в виде набора преобразований, каждое из которых обрабатывает лишь часть элементов блока:
$$s(x^{(1)}, ..., x^{(2n)}) = \big(s_1(x^{(1)}, ..., x^{(u)}), ..., s_d(x^{(2n-u+1)}, ..., x^{(2n)})\big) \tag{50}$$
где $d \mid 2n, u = 2n/d$. Число S-боксов d выбирается как компромисс между криптографическими кач-вами и сложностью реализации.
3. Свойства раундовых функций должны затруднять получение ключа с помощью известных методов криптоанализа (например, линейного или дифференциального)
4. Перемешивающие слои раундовой функции должны обеспечивать такие связи между входными и выходными битами S-боксов, что выполняются условия:
   - каждый S-бокс удовлетворяет критерию лавнного эффекта (любой выходной бит зависит от всех входных битов)

- на следующем раунде совокупность входных битов S-бокса зависит от выходов нескольких S-боксов предыдущего раунда

DES - 16-раундовый шифр Фейстеля. Входной блок имеет размер 64 бита, ключ - 56 бит. Раундовые ключи имеют размер 48 бит. Входное и выходное отображения от ключа не зависят и $\pi = \delta^{-1} \cdot T^{32}$

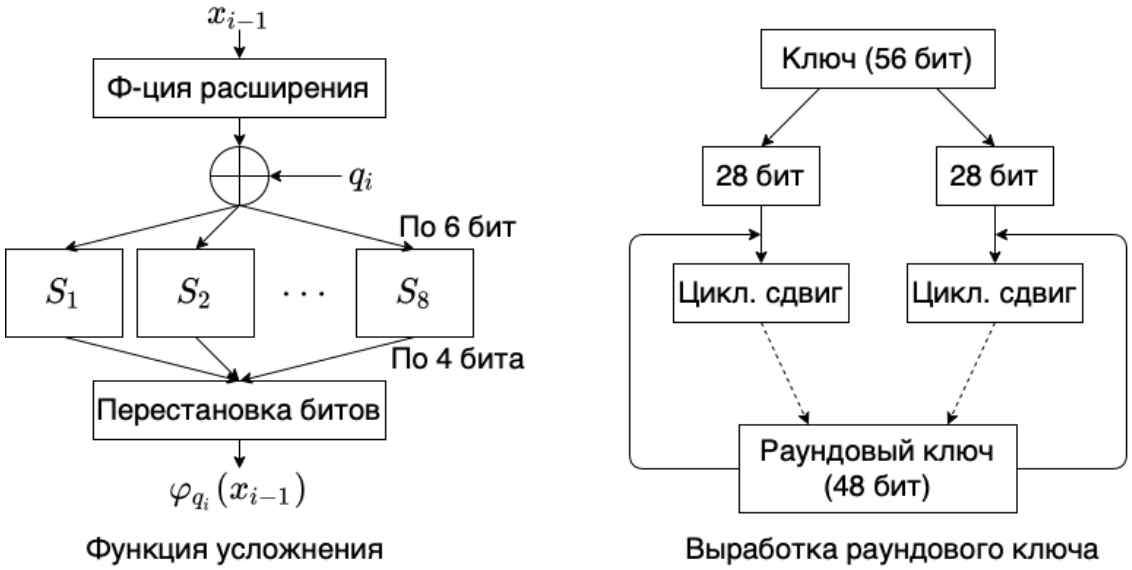
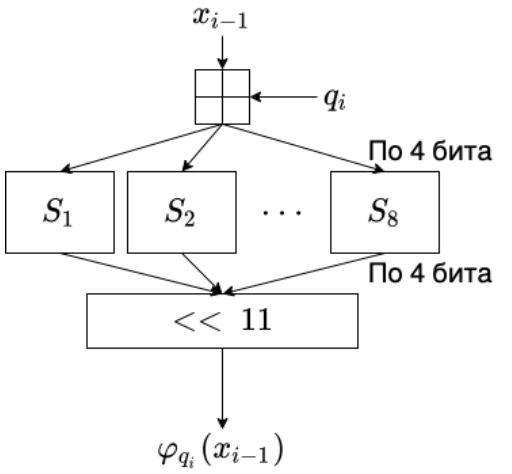


Рис. 5: DES.

Магма - 32-раундовый шифр Фейстеля. Входной блок имеет размер 64 бита, ключ - 256 бит. Раундовые ключи имеют размер 32 бита. $\delta = e, \pi = T^{32}$



$$
\begin{array}{llll}
q_1 = k_1 & q_9 = k_1 & q_{17} = k_1 & q_{25} = k_8 \\
q_2 = k_2 & q_{10} = k_2 & q_{18} = k_2 & q_{26} = k_7 \\
q_3 = k_3 & q_{11} = k_3 & q_{19} = k_3 & q_{27} = k_6 \\
q_4 = k_4 & q_{12} = k_4 & q_{20} = k_4 & q_{28} = k_5 \\
q_5 = k_5 & q_{13} = k_5 & q_{21} = k_5 & q_{29} = k_4 \\
q_6 = k_6 & q_{14} = k_6 & q_{22} = k_6 & q_{30} = k_3 \\
q_7 = k_7 & q_{15} = k_7 & q_{23} = k_7 & q_{31} = k_2 \\
q_8 = k_8 & q_{16} = k_8 & q_{24} = k_8 & q_{32} = k_1
\end{array}
$$

$$k = k_1||k_2||k_3||k_4||k_5||k_6||k_7||k_8$$

Выработка раундового ключа

Рис. 6: Магма.

17 Слабый ключ итеративного СБШ, μ-слабый ключ итеративного СБШ. Теорема о количестве раундов СБШ со слабым ключом, следствие. Теорема об особенностях подстановки шифра Фейстеля при использовании слабого ключа. Количество слабых ключей алгоритмов DES и ГОСТ 28147-89.

Ключ ИСБШ называется μ-слабым, при котором среди раундовых ключей ровно μ различных. Слабым ключом ИСБШ называется ключ, при котором все раундовые ключи являются одинаковыми.

Теорема: Пусть k - слабый ключ r-раундового ИСБШ, $d = \operatorname{ord} \varphi_q$, τ - остаток от деления r на d. В этом случае ИСБШ с ключом k является τ-цикловым.

Доказательство: так как k - слабый ключ, то алгоритм зашифрования выглядит следующим образом:

$$E_k = \pi_{q_{r+1}} \cdot \varphi_q^r \cdot \delta_{q_0} \tag{51}$$

Исходя из условий теоремы верно, что: $\varphi_q^r = \varphi_q^\tau$. Теорема доказана.

Следствие: Если $d \mid r$, а δ_{q_0} и $\pi_{q_{r+1}}$ взаимнообратные, то E_k - тождественная подстановка.

Теорема: Пусть k - слабый ключ $2r$-раундового шифра Фейстеля, $q_0 = q_{r+1}$, $\pi_{q_0} = \delta_{q_0}^{-1} \cdot T^n$. Тогда E_k - инволюция и имеет 2^n неподвижных элементов.

Доказательство: алгоритм зашифрования:

$$E_k = \delta_{q_0}^{-1} \cdot T^n \cdot \varphi_q^{2r} \cdot \delta_{q_0} \tag{52}$$

Несложно увидеть, что E_k в данном случае - инволюция, так как расшифрование отличается от зашифрования применением раундовых ключей в обратном порядке.

Пусть $\delta_{q_0}((a_1, a_2)) = (x_1, x_2)$. (a_1, a_2) - неподвижный элемент $E_k \iff (x_1, x_2)$ - неподвижный элемент $T^n \cdot \varphi_q^{2r}$. Или что равносильно: (x_1, x_2) - корень уравнения:

$$\varphi_q^r((x_1, x_2)) = \varphi_q^r \cdot T^n((x_1, x_2)) \tag{53}$$

Что равносильно:

$$(x_1, x_2) = T^n((x_1, x_2)) \tag{54}$$

А в силу определения: $T^n((x_1, x_2)) = (x_2, x_1)$

Таким образом, число неподвижных эл-тов подстановки E_k равно кол-ву различных эл-тов вида $(x, x), x \in V_n$, т.е. 2^n. Теорема доказана.

DES имеет 4 слабых ключа, ГОСТ-28147-89 - $2^3 2$ слабых ключа.

18 Режимы шифрования и их особенности: простая замена, сцепление блоков шифртекста, гаммирование с обратной связью по шифртексту, гаммирование с внутренней обратной связью. Замечание об использовании режима простой замены. Замечание об использовании вектора инициализации.

Режим простой замены (ECB):

$$y_i = E_k(x_i) \tag{55}$$

$$x_i = E_k^{-1}(y_i) \tag{56}$$

1. Замены и перестановки блоков шифртекста не нарушают корректность расшифрования
2. Зашифрованные на одном ключе одинаковые блоки открытого текста переходят в одинаковые блоки шифртекста независимо от позиции
3. Изменение одного бита в блоке шифртекста приводит к изменению в среднем половины соответствующего блока открытого текста без влияния на остальные блоки
4. Если бит шифртекста удален или добавлен, то соответствующий и все последующие блоки будут расшифрованы неверно
5. Подходит для зашифрования только коротких сообщений (1 блок)

Режим простой замены с зацеплением (CBC):

$$y_i = E_k(x_i \oplus y_{i-1}), y_0 = IV \tag{57}$$

$$x_i = E_k^{-1}(y_i) \oplus y_{i-1}, y_0 = IV \tag{58}$$

1. Изменение одного бита в блоке шифртекста приводит к изменению в среднем половины соответствующего блока открытого текста и изменению соответствующего бита в следующем блоке
2. Неустойчив к ошибкам синхронизации
3. Синхропосылка может передаваться в открытом виде. Необходимо избегать повтора синхропосылки для одного ключа. Она должна выбираться случайно, равновероятно и независимо от ключа.

Режим гаммирования с обратной связью (OFB):

$$y_i = x_i \oplus E_k(\gamma_{i-1}), \gamma_0 = IV \tag{59}$$

$$x_i = y_i \oplus E_k(\gamma_{i-1}), \gamma_0 = IV \tag{60}$$

В наиболее общем виде из полученного блока гаммы выбираются m бит и накладываются на открытый текст.

1. Ошибки не распростаняются (гамма генерируется автономно)

2. Неустойчив к ошибкам синхронизации

Режим гаммирования с обратной связью по шифртексту (CFB):

$$y_i = x_i \oplus E_k(y_{i-1}), y_0 = IV \tag{61}$$

$$x_i = y_i \oplus E_k(y_{i-1}), y_0 = IV \tag{62}$$

В наиболее общем виде из полученного блока гаммы выбираются m бит и накладываются на открытый текст.

1. Не требует реализации функции расшифрования, а функция зашифрования может быть реализована в виде хэш-фнкции $h : V_n \to V_m$
2. Искажение i-го бита шифртекста приводит к искажению соответствующего бита в открытом тексте и около половины бит в последующих l блоках: $\lfloor \frac{n}{m} \rfloor \leq l \leq \lceil \frac{n}{m} \rceil$
3. Сам восстанавливается после ошибок синхронизации