11 Поточные криптосистемы

11.1 Поточные криптосистемы

Напомним наше определение поточной криптосистемы. Пусть имеется слово $X \in A^*$ длины $|X| = T$. Для зашифрования данного слова на ключе $\theta \in \Theta$ выполняются следующие действия:

1. Выбирается криптосистема $\langle \Gamma, A, \mathcal{Y}, E, D \rangle$.
2. По θ строится слово $\gamma \in \Gamma^T$ (*гамма*).
3. Зашифрование выполняется по правилу:

$$X = x_1 x_2 \dots x_T \mapsto E_{\gamma_1}(x_1) E_{\gamma_2}(x_2) \dots E_{\gamma_T}(x_T).$$

На практике используется алфавит $A = \{0,1\}^n$ (n — невелико, в большинстве случаев $n = 1$ или 8), устанавливается $\Gamma = A$ и применяются простые правила зашифрования и расшифрования:

$$E_\gamma(x) = D_\gamma(x) = x \oplus \gamma.$$

Поэтому важность представляет, в первую очередь, алгоритм построения гаммы $\gamma_1 \gamma_2 \dots$ по ключу θ (шаг 2). В связи этим будем сужать определение поточной криптосистемы:

Определение 11.1. Поточной криптосистемой будем называть совокупность $G = \{G_\theta \colon \theta \in \Theta\} \subset A^\infty$ последовательностей (гамм) бесконечной длины в алфавите A. □

Рассмотренные нами ранее условия криптоаналитических атак на блочные криптосистемы при переходе к поточным криптосистемам сохраняются. Атаки при известном, выбранном и выбираемом открытом текстах для поточных криптосистем эквивалентны. В условиях этих атак криптоаналитику становится известным отрезок $\gamma_1, \dots, \gamma_T$ последовательности G_θ, требуется решить одну из следующих задач:

(S1) определить ключ θ;

(S2) не определяя θ, построить алгоритм вычисления $\gamma_{T+1}, \gamma_{T+2}, \dots$;

(S3) удостовериться, что наблюдается отрезок последовательности из G.

11.2 Конечные автоматы

Функционирование поточной криптосистемы G удобно описывать с помощью модели конечного автомата.

Автомат задается следующими элементами:

(i) $\mathcal{S}$ — множество внутренних состояний;

(ii) A — выходной алфавит;

(iii) $\varphi \colon \mathcal{S} \to \mathcal{S}$ — функция перехода (между состояниями);

(iv) $\pi \colon \mathcal{S} \to A$ — функция выхода.

Дополнительный криптографический элемент автомата:

(v) функция загрузки ключа $\psi \colon \Theta \to \mathcal{S}$.

Функционирование автомата:

$$S_0 = \psi(\theta), \quad S_t = \varphi(S_{t-1}), \quad \gamma_t = \pi(S_t), \quad t = 1, 2, \dots.$$

Пример 11.1 (RC4)**.** Поточная криптосистема RC4 используется во многих приложениях, например, при защите «цифровых прав» PDF-файлов и в протоколах беспроводного доступа.

Элементы криптосистемы:

– ключ $\theta \in \mathbb{Z}_{256}^l$, заданный таблицей значений $\theta[0], \ldots, \theta[l-1]$;

– состояние $(s, i, j) \in \mathcal{S} = S(\mathbb{Z}_{256}) \times \mathbb{Z}_{256} \times \mathbb{Z}_{256}$, подстановка s задается таблицей значений $s[0], \ldots, s[255]$;

– выходной алфавит $A = \mathbb{Z}_{256}$;

– функция загрузки ключа (алгоритмическое определение):

а) для $u = 0, \ldots, 255$ установить $s[u] \leftarrow u$;

б) установить $v \leftarrow 0$;

в) для $u = 0, \ldots, 255$ выполнить: $v \leftarrow v + s[u] + \theta[u \bmod l]$, $s[u] \leftrightarrow s[v]$;

г) установить $i \leftarrow 0$, $j \leftarrow 0$;

– функция перехода (алгоритмическое определение):

а) $i \leftarrow i + 1$;

б) $j \leftarrow j + s[i]$,

в) $s[i] \leftrightarrow s[j]$;

– функция выхода: $\pi(s, i, j) = s[s[i] + s[j]]$. □

11.3 РСЛОС

Следующий автомат получил наибольшее распространение при построении поточных криптосистем:

– состояние $S_t \in \mathcal{S} = \mathbb{F}_2^n$ (вектор-строка),

– функция перехода: $S_t = \varphi(S_{t-1}) = S_{t-1}M$, где M — матрица порядка n над полем $\mathbb{F}_2$ вида

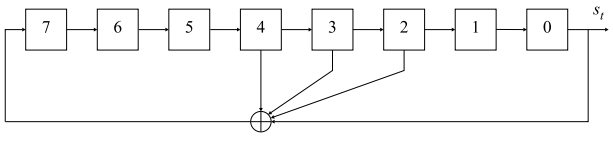
$$M = \begin{pmatrix} 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & \ldots & 0 & a_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & a_{n-1} \end{pmatrix}, \quad a_i \in \mathbb{F}_2,$$

– выходной алфавит $\mathbb{F}_2 = \{0, 1\}$;

– функция выхода: $s_t = \pi(S_t) = S_{t,1}$ (первая координата вектора S_t).

Автомат, который функционирует по таким правилам получил название *регистра сдвига с линейной обратной связью* (РСЛОС).

Пример 11.2 (РСЛОС). Пусть $n = 8$ и $(a_0, \ldots, a_7) = (1, 0, 1, 1, 1, 0, 0, 0)$. Соответствующий РСЛОС представлен на следующем рисунке:



(для других автоматов в РСЛОС меняются длины регистров и коэффициенты обратной связи a_i). □

Выходная последовательность (s_t) РСЛОС может быть задана следующим соотношением:

$$s_{t+n} = a_{n-1}s_{t+n-1} + \ldots + a_1 s_{t+1} + a_0 s_t, \quad t = 1, 2, \ldots, \qquad (\star)$$

с начальными условиями $(s_1, s_2, \ldots, s_n) = S_0$.

Определение 11.2. Последовательность $(\star)$ называется *линейной рекуррентной последовательностью* (л.р.п.) порядка n (над полем $\mathbb{F}_2$). □

Пример 11.3 (числа Фибоначчи). Вместо л.р.п. над полем $\mathbb{F}_2$ можно рассмотреть л.р.п. над произвольным полем или даже над произвольным кольцом. Последовательность

$$s_{t+2} = s_{t+1} + s_t, \quad t = 1, 2 \ldots, \quad s_1 = s_2 = 1,$$

над кольцом $\mathbb{Z}$ получила название последовательности Фибоначчи (1202 г.). □

Из курса линейной алгебры известно, что характеристический многочлен матрицы M имеет вид

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{F}_2[x].$$

Данный многочлен называется также *характеристическим многочленом* л.р.п. $s_1, s_2, \ldots$. Матрица M при этом называется *сопровождающей матрицей* $f(x)$.

11.4 Функция «след»

Определение 11.3. Пусть K — поле из q элементов и F — расширение K степени m. *Следом* элемента $a \in F$ над K называется величина

$$\mathrm{Tr}_{F/K}(a) = a + a^q + a^{q^2} + \ldots + a^{q^{m-1}}.$$

Если K — простое подполе F, то $\mathrm{Tr}_{F/K}(a)$ называется *абсолютным следом* и обозначается просто $\mathrm{Tr}_F(a)$ или даже $\mathrm{Tr}(a)$. □

Теорема 11.1 (свойства следа). Функция $\mathrm{Tr}_{F/K}$ обладает следующими свойствами:

(1) $\mathrm{Tr}_{F/K}(a^q) = \mathrm{Tr}_{F/K}(a)^q = \mathrm{Tr}_{F/K}(a)$ для всех $a \in F$;

(2) $\mathrm{Tr}_{F/K}(a) \in K$ для всех $a \in F$;

(3) $\mathrm{Tr}_{F/K}(a+b) = \mathrm{Tr}_{F/K}(a) + \mathrm{Tr}_{F/K}(b)$ для всех $a, b \in F$;

(4) $\mathrm{Tr}_{F/K}(\alpha a) = \alpha \,\mathrm{Tr}_{F/K}(a)$ для всех $\alpha \in K$, $a \in F$;

(5) $\mathrm{Tr}_{F/K}$ является сюръективным отображением $F \to K$ (отображением “на”).

Лемма 11.1. Для всех $\alpha \in K$ выполняется: $\alpha^q = \alpha$. Если для $\alpha \in F$ выполняется $\alpha^q = \alpha$, то $\alpha \in K$.

Доказательство. Равенство $\alpha^q = \alpha$ очевидно выполняется для $\alpha = 0$. Для ненулевого α по теореме Лагранжа $\mathrm{ord}\,\alpha$ делит порядок $q-1$ мультипликативной группы K^*. Следовательно $\alpha^{q-1} = 1$ или $\alpha^q = \alpha$.

Все элементы K являются корнями многочлена $f(x) = x^q - x \in F[x]$. Если $f(\alpha) = 0$ для некоторого $\alpha \notin K$, то многочлен f степени q имеет $> q$ корней, что невозможно. □

Доказательство. **1.** Будем учитывать лемму о степени суммы ($(a+b)^q = a^q + b^q$) и тот факт, что $a^{q^m} = a$. Имеем

$$\mathrm{Tr}_{F/K}(a^q) = a^q + a^{q^2} + \ldots + a^{q^{m-1}} + a^{q^m} = \begin{cases} a^q + a^{q^2} + \ldots + a^{q^{m-1}} + a = \mathrm{Tr}_{F/K}(a), \\ (a + a^q + \ldots + a^{q^{m-1}})^q = \mathrm{Tr}_{F/K}(a)^q. \end{cases}$$

2. Согласно (1) $\mathrm{Tr}_{F/K}(a)^q - \mathrm{Tr}_{F/K}(a) = 0$. Следовательно, элемент $\mathrm{Tr}_{F/K}(a)$ лежит в подполе из q элементов, т. е. в K.

3. Следует из леммы о степени суммы.

4. Проверяется непосредственно с учетом того, что $\alpha^q = \alpha$.

5. С учетом (4) достаточно показать, что имеется элемент $a \in F$ такой, что $\mathrm{Tr}_{F/K}(a) \neq 0$. Ясно, что $\mathrm{Tr}_{F/K}(a) = 0$ только если a является корнем многочлена $x + x^q + x^{q^2} + \ldots + x^{q^{m-1}} \in K[x]$. Данный многочлен может иметь не более q^{m-1} корней в F. Но $|F| = q^m$ и нужный нам элемент a существует. □

Пусть F и K рассматриваются как векторные пространства над полем K (размерности m и 1 соответственно). Доказанная теорема означает, что отображение $\mathrm{Tr}_{F/K}$ является линейным отображением F на K. Более того,

Теорема 11.2. Линейными отображениями $F \to K$ являются отображения вида

$$L_b\colon a \mapsto \mathrm{Tr}_{F/K}(ab), \quad b \in F,$$

и только они.

Доказательство. Всего имеется q^m различных линейных отображений $F \to K$ (действие линейного отображения $L\colon F \to K$ однозначно задается выбором элементов $L(a_1), \ldots, L(a_m)$, где $a_1, \ldots, a_m$ — базис F над K.

Отображения L_b и L_c различны для $b \neq c$ (если $L_b(a(b-c)^{-1}) = L_c(a(b-c)^{-1})$ для всех $a \in F$, то $Tr_{F/K}(a) = 0$ для всех a, противоречие с п. (5) теоремы), следовательно, только такими отображениями исчерпываются линейные. □

11.5 РСЛОС и функция «след»

Поле $\mathbb{F}_{q=p^n}$ мы строили как факторкольцо $\mathbb{F}_p[x](f(x))$, где $f(x) \in \mathbb{F}_p[x]$ — неприводимый многочлен степени. Элементами факторкольца являются многочлены из $\mathbb{F}_p[x]$ степени $< n$. При этом многочлен $\alpha = x$ является корнем $f(x)$: $f(\alpha) = f(x) \equiv 0 \pmod{f(x)}$.

Корнями f в $\mathbb{F}_q$ являются также элементы $\alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{n-1}}$. Действительно, по лемме о степени суммы

$$f(\alpha^{p^i}) = f(\alpha)^{p^i} = 0.$$

Лемма 11.2 (о базисе). Набор $\alpha, \alpha^2, \ldots, \alpha^n$ является базисом $\mathbb{F}_q$ над $\mathbb{F}_p$.

Доказательство. Предположим, что указанные элементы линейно зависимы: $\alpha \sum_{i=0}^{n-1} b_i \alpha^i = 0$, где $(b_0, b_1, \ldots, b_{n-1}) \neq (0, 0, \ldots, 0)$. Тогда α — корень ненулевого многочлена $\sum_{i=0}^{n-1} b_i x^i$.

Пусть $g \in \mathbb{F}_p[x]$ — ненулевой многочлен, для которого α является корнем и который имеет минимальную степень среди всех таких многочленов. Сказанное выше означает, что $\deg g < n$. Выполним деление f на g:

$$f(x) = g(x)h(x) + r(x), \quad \deg r < \deg g.$$

Тогда $r(\alpha) = 0$ и по построению $r = 0$. Но тогда f не является неприводимым. Противоречие. □

Теорема 11.3 (РСЛОС и функция «след»). Пусть характеристический многочлен f л.р.п. (s_t) неприводим и α — корень f в расширении $\mathbb{F}_{2^n} \cong \mathbb{F}_2[x]/(f(x))$ поля $\mathbb{F}_2$. Тогда существует однозначно определенный элемент $b \in \mathbb{F}_{2^n}$ такой, что

$$s_t = \mathrm{Tr}(b\alpha^t), \quad t = 1, 2, \ldots.$$

Доказательство. Так как элементы $\{\alpha, \ldots, \alpha^n\}$ образуют базис $\mathbb{F}_{2^n}$ над $\mathbb{F}_2$, то существует однозначно определенное линейное отображение $L\colon \mathbb{F}_{2^n} \to \mathbb{F}_2$ такое, что

$$L(\alpha^t) = s_t, \quad t = 1, 2, \ldots, n.$$

Но из предыдущей теоремы следует, что имеется однозначно определенный элемент b такой, что $L(a) = \mathrm{Tr}(ba)$ для всех $a \in \mathbb{F}_{2^n}$. Поэтому

$$s_t = \mathrm{Tr}(b\alpha^t), \quad t = 1, 2, \ldots, n.$$

Остается проверить $(\star)$. Для каждого $t = 1, 2, \ldots$ имеем

$$\begin{aligned} s_{t+n} - a_{n-1}s_{t+n-1} - \ldots - a_1 s_{t+1} - a_0 s_t &= \mathrm{Tr}(b\alpha^{t+n}) - \sum_{i=0}^{n-1} a_i \,\mathrm{Tr}(b\alpha^{t+i}) = \\ &= \mathrm{Tr}(b\alpha^t(\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0)) = \\ &= \mathrm{Tr}(b\alpha^t f(\alpha)) = 0, \end{aligned}$$

что и требовалось установить. □

Доказанная теорема позволяет построить альтернативный РСЛОС автомат, формирующий ту же л.р.п.: $\mathcal{S} = \mathbb{F}_{2^n}$, $S_0 = b$, $\varphi(S) = S\alpha$, $\pi(S) = \mathrm{Tr}(S)$.

11.6 Период л.р.п.

Множество состояний $\mathcal{S}$ конечного автомата конечно и при функционировании автомата рано или поздно встретятся два одинаковых внутренних состояния: $S_t = S_\tau$, $t \neq \tau$. Данное совпадение приведет к совпадениям состояний $S_{t+1} = \varphi(S_t) = \varphi(S_\tau) = S_{\tau+1}$, $S_{t+2} = S_{\tau+2}, \ldots$ и совпадениям выходных символов

$$\gamma_t = \pi(S_t) = \pi(S_\tau) = \gamma_\tau, \quad \gamma_{t+1} = \gamma_{\tau+1}, \quad \gamma_{t+2} = \gamma_{\tau+2}, \ldots$$

Таким образом, выходная последовательность всякого конечного автомата оказывается периодической. При использовании автомата для криптографических нужд желательно, чтобы период выходной последовательности был как можно больше (см., напр., задачу S2).

Определение 11.4. Последовательность $\gamma_1, \gamma_2, \ldots$ называется *периодической*, если найдутся целые $t_0 \geqslant 0$ и $r > 0$ такие, что

$$\gamma_{t+r} = \gamma_t$$

для всех $t > t_0$. При этом r называется *периодом* последовательности, а наименьший из всех возможных периодов называется *минимальным периодом*. □

Определение 11.5. Пусть $s_1, s_2, \ldots$ — периодическая последовательность с минимальным периодом r. Наименьшее целое $t_0 \geqslant 0$ такое, что $s_{t+r} = s_t$ для всех $t > t_0$ называется *предпериодом* последовательности. Периодическая последовательность называется *чисто периодической*, если ее предпериод $= 0$. □

Пример 11.4. Рассмотрим последовательность десятичных знаков дроби

$$\frac{11}{12} = 0.91666\ldots.$$

Период данной последовательности — 1, предпериод — 2. □

Перейдем к анализу периода л.р.п. (s_t) порядка n с неприводимым характеристическим многочленом $f(x)$. При выборе нулевых начальных условий $s_1 = s_2 = \ldots = s_n = 0$ вся последовательность (s_t) также оказывается нулевой. Будем отбрасывать данный тривиальный случай и рассматривать только л.р.п. с ненулевыми начальными условиями.

Пример 11.5. Пусть $f(x) = x^4 + x + 1$, $g(x) = x^4 + x^3 + x^2 + x + 1$. Построим л.р.п. порядка 4 с характеристическими многочленами f и g и начальными условиями: $s_1 = s_2 = s_3 = 0$, $s_4 = 1$. Последовательности задаются рекуррентными соотношениями

$$s_{t+4} = s_{t+1} + s_t, \quad s_{t+4} = s_{t+3} + s_{t+2} + s_{t+1} + s_t,$$

выглядят следующим образом:

$$0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, \ldots,$$
$$0, 0, 0, 1, 1, 0, 0, 0, 1, \ldots,$$

и имеют период 15 и 5 соответственно. Наша ближайшая задача — связать период л.р.п. со свойствами характеристических многочленов f и g. □

Теорема 11.4 (о периоде л.р.п.). Ненулевая л.р.п. (s_t) с неприводимым характеристическим многочленом f является чисто периодической последовательностью с минимальным периодом $\operatorname{ord}\alpha$, где α — корень f в некотором расширении $\mathbb{F}_2$.

Доказательство. Пусть r — период (s_t). Тогда

$$s_{t+r} - s_t = \operatorname{Tr}(b\alpha^t(\alpha^r - 1)) = 0, \quad t \geqslant t_0.$$

Поскольку α^t пробегают все элементы базиса $\mathbb{F}_{2^n}$ над $\mathbb{F}_2$, $b \neq 0$ и функция Tr задает сюръективное отображение на $\mathbb{F}_2$, последнее возможно тогда и только тогда, когда $\alpha^r = 1$. Поэтому минимальный период (s_t) совпадает с $\operatorname{ord}\alpha$ — минимальным r таким, что $\alpha^r = 1$. □

11.7 Порядок многочлена

Определение 11.6. Пусть $f \in \mathbb{F}_2[x]$ и $f(0) \neq 0$. *Порядком* $\operatorname{ord} f$ многочлена f называется минимальное натуральное e для которого

$$f(x) \mid x^e - 1.$$

Теорема 11.5 (о порядке многочлена). Пусть $f \in \mathbb{F}_2[x]$ — неприводимый многочлен степени n и $f(0) \neq 0$ (т. е. $f(x) \neq x$). Тогда $\operatorname{ord} f = \operatorname{ord} \alpha$, где α — любой из корней f в поле $\mathbb{F}_{2^n}$. Более того, $\operatorname{ord} f \mid 2^n - 1$.

Доказательство. Нужный результат следует из того, что равенство $\alpha^e = 1$ выполняется тогда и только тогда, когда $f(x) \mid x^e - 1$. Действительно, выполним деление:

$$x^e - 1 = f(x)g(x) + r(x), \quad \deg r < n.$$

Подставляя в обе части $x = \alpha$, получаем $r(\alpha) = 0$. Но это возможно тогда и только тогда, когда $r = 0$ (см. доказательство леммы о базисе), т. е. $f(x) \mid x^e - 1$.

Последнее равенство следует из того, что

$$\operatorname{ord} \alpha \mid (\text{порядок } \mathbb{F}_{2^n}^*) = 2^n - 1$$

(по теореме Лагранжа). □

Упражнение 11.1 (⋆). Предложить алгоритм определения $\operatorname{ord} f$ при известной факторизации числа $2^{\deg f} - 1$. □

Определение 11.7. Неприводимый многочлен $f(x) \in \mathbb{F}_2[x]$, отличный от x, называется *примитивным*, если $\operatorname{ord} f = 2^{\deg f} - 1$. □

Как видим, максимальный период л.р.п. обеспечивается при выборе примитивного f. Ненулевые л.р.п. с примитивным характеристическим многочленом называют *m-последовательностями*.

Пример 11.6. Продолжая предыдущий пример: $\operatorname{ord} f = 15$, $\operatorname{ord} g = 5$, f — примитивный многочлен. □

Пример 11.7 (числа Мерсенна). Если $2^n - 1$ — простое число, то всякий неприводимый многочлен из кольца $\mathbb{F}_2[x]$ оказывается примитивным. Простые вида $2^n - 1$ получили название *простых Мерсенна*. В августе 2007 года объявлено о нахождении 47-го (не по порядковому номеру) простого Мерсенна:

$$2^{43\ 112\ 609} - 1.$$

Это самое большое из известных на сегодняшний день простых чисел (≈ 13 млн. десятичных знаков). □

11.8 Постулаты Голомба

Пусть $\gamma = \gamma_1, \gamma_2, \ldots$ — выходная последовательность конечного автомата, $\gamma_t \in \mathbb{F}_2$. Как мы уже говорили, последовательность γ является периодической. Пусть r — минимальный период γ. Для простоты полагаем, что предпериод равняется 0.

При решении задачи S2 Виктор пытается прогнозировать символы $\gamma_{T+1}, \ldots$ по известным символам $\gamma_1, \ldots, \gamma_T$. Если $T \geqslant r$, то Виктор может построить точный прогноз:

$$\gamma_t = \gamma_{t-r}, \quad t = T+1, \ldots.$$

К сожалению (для Виктора) на практике r велико и $T \ll r$. Однако и в этом случае Виктор может строить нетривиальные (с меньшей чем $1/2$ частотой ошибок) прогнозы, используя статические особенности γ.

С. Голомб выдвинул три постулата, которым должны удовлетворять последовательности γ:

R1. На отрезке $\gamma_1, \ldots, \gamma_r$ число нулей незначительно отличается от числа единиц.

R2. На отрезке периода примерно половина серий имеет длину 1, четверть — длину 2, восьмая часть — длину 3 и далее (серией называется максимальная подпоследовательность из одинаковых символов).

R3. Значения автокорреляционной функции

$$C_\gamma(\tau) = \sum_{t=1}^{r} \chi(\gamma_t + \gamma_{t+\tau})$$

близки к 0 для всех $\tau = 1, 2, \ldots, r-1$.

Покажем, что m-последовательность $s = (s_t)$ удовлетворяют постулатам Голомба R1 и R3. Период m-последовательности s равняется $r = 2^n - 1$.

R1. Вернемся к первоначальному определению л.р.п. с помощью РСЛОС:

$$S_t = S_{t-1}A, \quad s_t = S_{t,1}, \quad t = 1, 2, \ldots$$

Поскольку (s_t) — m-последовательность, векторы $S_1, \ldots, S_{2^n-1}$ различны и, следовательно, пробегают $\mathbb{F}_2^n \setminus \{0\}$. Выходные символы $s_1, \ldots, s_{2^n-1}$ являются первыми координатами данных векторов и, таким образом, на отрезке $s_1, \ldots, s_{2^n-1}$ встречается 2^{n-1} единиц и $2^{n-1} - 1$ нулей.

R3. Для всякого $\tau \in \{1, \ldots, r-1\}$ последовательность

$$s_t^* = s_t + s_{t+\tau}, \quad t = 1, 2, \ldots$$

удовлетворяет тому же рекуррентному соотношению, что и исходная m-последовательность (s_t). Последовательность (s_t^*) не может быть нулевой, так как в противном случае

$$s_1 = s_{\tau+1}, \quad s_2 = s_{\tau+2}, \ldots, \quad s_n = s_{\tau+n}, \ldots$$

и период (s_t) равняется $\tau < r$, противоречие. Следовательно, (s_t^*) — m-последовательность и

$$C_s(\tau) = \sum_{t=1}^{2^n-1} \chi(s_t^*) = 2^{n-1}\chi(1) + (2^{n-1} - 1)\chi(0) = -1.$$

11.9 Генераторы на базе РСЛОС

Пусть имеется один или несколько РСЛОС. Всюду далее будем предполагать, что в регистрах используются ненулевые начальные состояния и характерестические многочлены являются примитивными, ıе РСЛОС выдают m-последовательности.

Будем нумеровать регистры от 1 до d и при $d > 1$ помечать элементы i-го РСЛОС верхним индексом (напр., $(s_t^{(i)})$ — выходная л.р.п. соответствующего регистра).

Фильтрующий генератор ($d = 1$). Пусть $g \in \mathcal{F}_n$ — произвольная булева функция. Правило определения выходного символа

$$s_t = S_{t,1}, \quad t = 1, 2, \ldots$$

заменяется на правило

$$\gamma_t = g(S_t).$$

Комбинирующий генератор (d — произвольно). Выходные последовательности РСЛОС обрабатываются функцией $g \in \mathcal{F}_d$:

$$\gamma_t = g(s_t^{(1)}, \ldots, s_t^{(d)}), \quad t = 1, 2, \ldots.$$

Пример 11.8 (генератор Геффе). В комбинирующем генераторе Геффе $d = 3$ и $f(x_1, x_2, x_3) = x_1x_2 + (x_1+1)x_3$: выходной символ первого регистра управляет выбором между выходными символами второго или третьего регистров.□

Неравномерное движение. В этом случае выходные символы РСЛОС$^{(i)}$ управляют выполнением преобразований на РСЛОС$^{(j)}$ — автомат РСЛОС$^{(j)}$ может либо выполнять стандартное рекуррентное преобразование (умножение вектора состояния $S_t^{(j)}$ на сопровождающую матрицу характеристического многочлена $A^{(j)}$, *шаг*), либо простаивать ($S_{t+1}^{(j)} = S_t^{(j)}$, *стоп*).

Пример 11.9 (поточная криптосистема A5/1). Для защиты голосовых данных в сетях GSM используется поточная криптосистема A5/1. Криптосистема построена на базе трех РСЛОС с использованием техники неравномерного движения. Регистры сдвига — 19-, 22- и 23-разрядные. Начальное заполнение регистров определяется на основании ключа $\theta \in \mathbb{F}_2^{64}$, $64 = 19 + 22 + 23$.

Используется отображение $F\colon \mathbb{F}_2^3 \to \mathbb{F}_2^3$. Значения $(y_1, y_2, y_3) = F(x_1, x_2, x_3)$ определяются по следующей таблице:

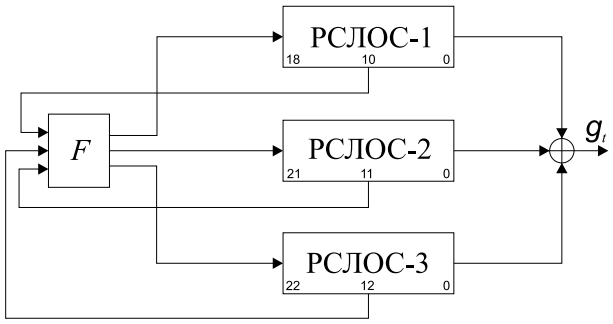
x_1	x_2	x_3	y_1	y_2	y_3
0	0	0	1	1	1
0	0	1	1	1	0
0	1	0	1	0	1
0	1	1	0	1	1
1	0	0	0	1	1
1	0	1	1	0	1
1	1	0	1	1	0
1	1	1	1	1	1

Действие F можно интерпретировать следующим образом: если в векторе (x_1, x_2, x_3) совпадают все координаты, то $y_1 = y_2 = y_3 = 1$. Если же $x_i = x_j \neq x_k$, то $y_i = y_j = 1$, $y_k = 0$ (правило большинства).

В фиксированных разрядах каждого РСЛОС снимаются биты x_1, x_2, x_3, которые подаются на вход функции F. Выходные биты y_1, y_2, y_3 определяют шаг или простой соответствующих РСЛОС.

Выходной символ определяется по правилу:

$$\gamma_t = S_{t,1}^{(1)} + S_{t,1}^{(3)} + S_{t,1}^{(3)}, \quad t = 1, 2, \ldots.$$



□

Сжимающий генератор ($d = 2$). Выходная последовательность РСЛОС$^{(1)}$ управляет выбором выходных символов РСЛОС$^{(2)}$:

$$\gamma_t = s_{\tau_t}^{(2)},$$

где τ_t — номер t-й единицы в последовательности $s_1^{(1)}, s_2^{(1)}, \ldots$.

Самосжимающий генератор ($d = 1$). Выходная последовательность разбивается на пары

$$(s_1, s_2), (s_3, s_4), \ldots.$$

Пары $(0, a)$ игнорируются, а по паре $(1, a)$ формируется очередной выходной символ $\gamma_t = a$.