12 Поточные криптосистемы

12.1 Поточные криптосистемы

Напомним наше определение поточной криптосистемы. Пусть имеется слово $X \in \{0,1\}^*$ длины $|X| = T$. Для зашифрования данного слова на ключе $K \in \mathcal{K}$ выполняются следующие действия:

1. Выбирается криптосистема $\langle \Gamma, \Sigma, \mathcal{Y}, E, D \rangle$.

2. По K строится слово $\gamma \in \Gamma^T$ (*гамма*).

3. Зашифрование выполняется по правилу:

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

На практике используется алфавит $\Sigma = \{0,1\}^n$ (n — невелико, в большинстве случаев $n = 1$ или 8), устанавливается $\Gamma = \Sigma$ 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 $\gamma_1 \gamma_2 \ldots$ по ключу K (шаг 2). В связи этим будем сужать определение поточной криптосистемы:

Определение 12.1. Поточной криптосистемой будем называть совокупность $G = \{G_K \colon K \in \mathcal{K}\} \subset \Sigma^\infty$ последовательностей (гамм) бесконечной длины в алфавите Σ. □

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 $\gamma_1, \ldots, \gamma_T$ последовательности G_K, требуется решить одну из следующих задач:

(S1) определить ключ K;

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

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

12.2 Конечные автоматы

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

Автомат задается следующими элементами:

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

(ii) Σ — выходной алфавит;

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

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

Дополнительный криптографический элемент автомата:

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

Функционирование автомата:

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

Пример 12.1 (RC4). Поточная криптосистема RC4 широко применялась в 1990-х. Элементы криптосистемы:

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

– 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 $\Sigma = \mathbb{Z}_{256}$;

– 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: $v \leftarrow v + s[u] + K[u \bmod l]$, $s[u] \leftrightarrow s[v]$;

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

12.3 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

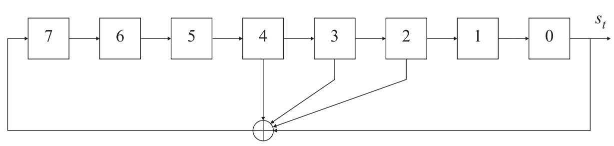
$$M = \begin{pmatrix} 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & \ldots & 0 & a_2 \\ \multicolumn{5}{c}{\dotfill} \\ 0 & 0 & \ldots & 1 & a_{n-1} \end{pmatrix}, \quad a_i \in \mathbb{F}_2,$$

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



Первый бит начального состояния записывается в ячейку с номером 0, второй бит — в ячейку с номером 1 и так далее. На каждом такте содержимое ячеек сдвигается влево, значение в ячейке с номером 0 выдается в качестве очередного выходного символа s_t. В освободившуюся ячейку (с номером 7) записывается сумма значений в ячейках с номерами $i \in \{0, 1, \ldots, 7\}$, для которых $a_i = 1$. Это и есть линейная обратная связь. □

Теорема 12.1. Выходная последовательность (s_t) РСЛОС может быть задана следующим соотношением:

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

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

Доказательство. Прямые расчеты. На первых n тактах из регистра с начальным состоянием S_0 выводятся символы $s_1, s_2, \ldots, s_n$. Каждый следующий символ — результат вычислений по формуле $(\star)$. □

Определение 12.2. Последовательность ($\star$) называется *линейной рекуррентной последовательностью* (л.р.п.) порядка n (над полем $\mathbb{F}_2$). $\square$

Пример 12.3 (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.). $\square$

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* $f(x)$.

12.4 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 n. 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 12.1 (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. $\square$

Теорема 12.2 (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

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

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

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

Согласно следствию из теоремы о функции «след» (пункт 5.9) имеется однозначно определенный элемент b такой, что $L(a) = \operatorname{Tr}(ba)$ для всех $a \in \mathbb{F}_{2^n}$. Поэтому

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

Остается проверить, что рекуррентное соотношение ($\star$) остается справедливым при подстановке $\operatorname{Tr}(b\alpha^t)$ вместо s_t. Для каждого $t = 1, 2, \ldots$ имеем:

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

что и требовалось показать. $\square$

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