УДК 519.92, 519.2

СОЛОВЕЙ О. В.

О МАРКОВСКИХ СЛУЧАЙНЫХ БЛУЖДАНИЯХ ДЛЯ ГЕНЕРАТОРОВ С ПРОРЕЖИВАНИЕМ

Рассматриваются регулярные цепи Маркова, матрица переходных вероятностей которых является матрицей-циркулянтом. Такие цепи описывают функционирование некоторых криптографических генераторов псевдослучайных чисел с прореживанием. Получены выражения для фундаментальной матрицы таких цепей, а также для матрицы средних времен достижения. Найденные выражения упрощают исследование периода и криптографических свойств генераторов с прореживанием.

Генераторы псевдослучайных чисел широко используются в криптографии [1, 2]. Они должны обладать хорошими криптографическими и статистическими свойствами. Одним из распространенных в литературе подходов к улучшению свойств генераторов является использование операции прореживания внутренних состояний генератора [2, 3].

Пусть имеется генератор G со множеством внутренних состояний Ω, пронумерованных от 0 до $n-1$, и функцией $\sigma : \Omega \to \Omega$ перехода между состояниями. Пусть σ является полноцикловой подстановкой, т. е. для $S \in \Omega$ образы $\sigma(S), \sigma^2(S) = \sigma(\sigma(S)), \ldots, \sigma^n(S)$ пробегают все Ω.

При обычной работе генератора G на основании выбранного начального состояния $S_0 \in \Omega$ определяется последовательность

$$S_{t+1} = \sigma(S_t), \quad t = 0, 1, \ldots \tag{1}$$

и текущее внутреннее состояние S_t используется для определения текущего выходного псевдослучайного числа [2, 3].

Прореживание (внутренних состояний G) состоит во введении дополнительной управляющей последовательности $d_0, d_1, d_2, \ldots \in \{0, 1, \ldots, n-1\}$ и замене правила (1) на правило

$$S_{t+1} = \sigma^{d_t}(S_t), \quad t = 0, 1, \ldots.$$

Пусть управляющая последовательность $d_0, d_1, d_2, \ldots$ является последовательностью независимых случайных величин с распределением вероятностей $\mathrm{P}\{d_t = k\} = p_k$, $k = 0, \ldots, n-1$. Тогда последовательность внутренних состояний $S_0, S_1, S_2, \ldots \in \Omega$ образует однородную цепь Маркова с матрицей вероятностей одношаговых переходов

$$P = \begin{pmatrix} p_0 & p_1 & \cdots & p_{n-1} & p_n \\ p_{n-1} & p_0 & \cdots & p_{n-1} & p_{n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ p_2 & p_3 & \cdots & p_0 & p_1 \\ p_1 & p_2 & \cdots & p_{n-1} & p_0 \end{pmatrix}. \tag{2}$$

Матрицу вида (2) называют матрицей-циркулянтом и обозначают $P = \mathrm{circ}(p_0, p_1, \ldots, p_{n-1})$. Далее все матрицы, если не сказано обратное, будут иметь размерность $n \times n$.

Пусть $\omega = \exp\{2\pi i / n\}$ – комплексный корень n-й степени из единицы, $\overline{\omega} = \exp\{-2\pi i / n\}$ – сопряженное к ω число, $F = (f_{kj})$ – матрица дискретного преобразования Фурье, $F^* = (f^*_{kj})$ – сопряженная к F матрица, где

$$f_{kj} = \frac{1}{\sqrt{n}}\omega^{kj}, \quad f^{*}_{kj} = \frac{1}{\sqrt{n}}\overline{\omega}^{kj}, \quad k, j = 0,\ldots,n-1.$$

Тогда для матрицы-циркулянта P справедливо разложение [4]:

$$P = F^{*}\Lambda F,$$

где $\Lambda = \mathrm{diag}(\lambda_0,\ldots,\lambda_{n-1})$ – диагональная матрица с элементами

$$\lambda_k = \sum_{j=0}^{n-1} p_j \overline{\omega}^{kj}, \quad k = 0,\ldots,n-1,$$

по главной диагонали.

При изучении свойств марковских последовательностей важную роль играют следующие матрицы [5].

1. Предельная матрица A. Для регулярной цепи Маркова $P^m \to A$ при $m \to \infty$. Каждая строка матрицы A представляет один и тот же вероятностный вектор $\alpha = (\alpha_0,\ldots,\alpha_{n-1})$. Вектор α задает вероятности находиться в каждом из состояний через большое число шагов.
2. Фундаментальная матрица

   $$Z = (E - (P\text{-}A))^{-1},$$

   где E – единичная матрица. С помощью матрицы Z вычисляется большинство важных характеристик регулярных цепей Маркова.
3. Матрица средних времен достижения

   $$M = (E - Z + J Z_{dg})D,$$

   где J – матрица, составленная из единиц; Z_{dg} – матрица, главная диагональ которой совпадает с главной диагональю Z, а прочие элементы равны нулю; $D = \mathrm{diag}(1/\alpha_0,\ldots,1/\alpha_{n-1})$. Элементы m_{kj} матрицы M в случае регулярных цепей Маркова задают среднее время, за которое процесс из k-го состояния впервые попадет в j-ое состояние.

Матрицы Z и M имеют важное значение при исследовании периода и криптографических свойств генераторов. Однако, при больших значениях n вычисление матриц Z и M по прямым формулам представляется затруднительным, а иногда и невозможным. Нами были получены формулы, которые упрощают вычисления.

Теорема. *Пусть $S_0, S_1, S_2, \ldots$ – регулярная цепь Маркова с матрицей вероятностей одношаговых переходов (2), тогда*

1) *предельная матрица* $A = \frac{1}{n}J$,
2) *фундаментальная матрица имеет вид*

   $$Z = F^{*}CF, \quad C = \mathrm{diag}\left(1, \frac{1}{1-\lambda_1},\ldots,\frac{1}{1-\lambda_{n-1}}\right),$$

3) *матрица средних времен достижения является матрицей-циркулянтом, т. е.* $M = \mathrm{circ}(m_0,\ldots,m_{n-1})$, *где*

   $$m_0 = n, \quad m_j = \sum_{k=1}^{n-1}\frac{1}{1-\lambda_k} - \sum_{k=1}^{n-1}\frac{\omega^{kj}}{1-\lambda_k}, \quad j = 1,\ldots,n-1.$$

В качестве примера, рассмотрим случай, когда у матрицы $P = \mathrm{circ}(p_0,\ldots,p_{n-1})$ элементы $p_1 = p_2 = 1/2$ и $p_0 = p_3 = p_4 = \ldots = p_{n-1} = 0$. Цепь Маркова с такой матрицей вероятностей одношаговых переходов описывает функционирование (1, 2)-шагового

генератора [6]. Покажем, что данная цепь является регулярной. Действительно, так как $p_1 > 0$, то процесс из любого состояния может попасть в любое, т. е. цепь неразложима. Далее, так как $p_1 = p_2 \neq 0$, то в любое состояние можно вернуться как за n, так и за $n-1$ шагов. Отсюда следует, что цепь состоит из одного циклического класса. Таким образом, нами установлена регулярность рассматриваемой цепи Маркова.

Далее, $\lambda_0 = 1$ и $\lambda_k = 1/2(\overline{\omega}^k + \overline{\omega}^{2k})$. Отсюда следует, что

$$\frac{1}{1-\lambda_k} = \frac{2}{2-\overline{\omega}^k - \overline{\omega}^{2k}} = \frac{2}{3}\left(\frac{1}{\overline{\omega}^k + 2} - \frac{1}{\overline{\omega}^k - 1}\right), \quad k = 1, \ldots, n-1,$$

и

$$m_j = \frac{2}{3}\sum_{k=1}^{n-1}\left(\frac{1}{\overline{\omega}^k + 2} - \frac{1}{\overline{\omega}^k - 1} - \frac{\omega^{kj}}{\overline{\omega}^k + 2} + \frac{\omega^{kj}}{\overline{\omega}^k - 1}\right).$$

Проводя несложные преобразования и используя полученные в работе [7] выражения для некоторых сумм Дедекинда, окончательно получаем

$$m_0 = n, \quad m_j = \frac{2}{3}\left(j + \frac{n(-2)^{n-j-1} - n(-2)^{n-1}}{(-2)^n - 1}\right), \quad j = 1, \ldots, n-1.$$

Библиографический список

1. Харин Ю. С., Агиевич С. В. Компьютерный практикум по математическим методам защиты информации: Учеб. пособие. Мн.: БГУ, 2001.

2. Rueppel R. Stream ciphers, Contemporary Cryptology: The Science of Information Integrity. New York: IEEE Press, 1991.

3. Соловей О. В., Харин Ю. С. Математические модели генераторов двоичных последовательностей с неравномерным движением регистров: обзор // Научно-практический журнал "Управление защитой информации", том 6, №2, 2002, стр. 77-83.

4. Gray R. M. Toeplitz and Circulant Matrices: A review. http://ee.stanford.edu/gray/toeplitz.pdf, 2002.

5. Кемени Дж., Снелл Дж. Конечные цепи Маркова. М.: Наука, 1970.

6. Варфоломеев А. А., Жуков А. Е., Пудовкина М. А. Поточные криптосистемы. Основные свойства и методы анализа стойкости. Учебное пособие. М.: ПАИМС, 2000.

7. Gessel I. M. Generating functions and generalized Dedenking sums // Electronic Journal of Combinatorics, v. 4, №2, 1997, R. 11.