О НЕКОТОРЫХ ПОДХОДАХ К МОДЕЛИРОВАНИЮ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ

Мальцев М. В, Палуха В. Ю, Харин Ю. С.

БГУ, Минск, Беларусь, e-mail: maltsew@mail.ru, vavan13@tut.by, kharin@bsu.by

Для обеспечения конфиденциальности и целостности данные при передаче через Internet подвергаются криптографическому преобразованию. Неотъемлемыми элементами криптографических преобразований являются криптографические генераторы. Поэтому актуальной является задача совершенствования криптографических генераторов, устранение их уязвимостей. В данной статье рассматриваются два подхода к данной проблеме.

Для обнаружения закономерностей в выходных последовательностях криптографических генераторов широко используются так называемые «малопараметрические» марковские модели [1, 2], поскольку число параметров для полносвязной цепи Маркова порядка s [3] увеличивается экспоненциально с ростом s. В статье рассматривается цепь Маркова условного порядка [4], также относящаяся к данному классу моделей. Для ее определиния нам понадобятся обозначения: $\mathbf{N}$ – множество натуральных чисел; $A=\{0, 1,\ldots, N-1\}$ – пространство состояний мощности $N \in \mathbf{N}$, $2 \le N < \infty$; $I\{C\}$ – индикатор события C; $J_n^m = (j_n, j_{n+1}, \mathbf{K}, j_m) \in A^{m-n+1}$, $m, n \in \mathbf{N}$, $m \ge n$, – мультииндекс; $L \in \{1, \mathbf{K}, s-1\}$, $K = N^L - 1$ – натуральные числа; $Q^{(1)}, \ldots, Q^{(M)}$ – семейство M $(1 \le M \le K+1)$ различных квадратных стохастических матриц порядка N: $Q^{(m)} = (q_{i,j}^{(m)})$, $0 \le q_{i,j}^{(m)} \le 1$, $\sum_{j \in A} q_{i,j}^{(m)} = 1$, $i, j \in A$, $1 \le m \le M$; $< J_n^m >= \sum_{k=n}^{m} N^{k-n} j_k$. Цепь Маркова s-го порядка $(2 \le s < \infty)$ $\{x_t \in A : t \in \mathbf{N}\}$ называется цепью Маркова условного порядка [4], если ее вероятности одношаговых переходов имеют вид: $\mathrm{P}\{x_t = j_{s+1} \mid x_{t-1} = j_s, \ldots, x_{t-s} = j_1\} = \sum_{k=0}^{K} I\{< J_{s-L+1}^s >= k\} q_{j_{b_k}, j_{s+1}}^{(m_k)}$, где $1 \le m_k \le M$, $1 \le b_k \le s - L$, $0 \le k \le K$, $\min_{0 \le k \le K} b_k = 1$. Последовательность элементов J_{s-L+1}^s называется базовым фрагментом памяти (БФП) случайной последовательности.

Для цепи Маркова условного порядка построены статистические оценки параметров $Q^{(i)}$, b_k, доказана их состоятельность. На основе асимптотических свойств оценок построен статистический тест для обнаружения отклонения наблюдаемой последовательности от модели равномерно распределенной случайной последовательности, часто называемой также «чисто случайной» последовательностью [5].

Рассмотрим далее подход к распознаванию генераторов двоичных последовательностей при помощи дискретного преобразования Фурье и нелинейного преобразования. Наблюдаемый дискретный временной ряд $x_1, x_2, \ldots, x_T$ длительности

$T = m \cdot n$ (m и n – заданные натуральные числа, $n > m$) разбивается на n фрагментов $X_1, \ldots, X_n$ длины m. Каждый фрагмент подвергается дискретному преобразованию Фурье (ДПФ): $X_i \xrightarrow{ДФП} Y_i = (y_{i1}, \mathbf{K}, y_{im}) \in \mathbf{R}^m, i = 1, \mathbf{K}, n$. Далее вычисляются величины $U_i = (u_{ik})$ при помощи нелинейного преобразования следующего вида $u_1 = y_1$, $u_i = y_i^2$, $i = 2, \ldots, m$. Для распознавания криптографических генераторов использовались статистики, основанные на собственных векторах $\hat{v}_m$ выборочной ковариационной матрицы $\hat{\Sigma}$, построенной по выборке $U_1, \ldots, U_n$: $t_i^{(j)} = T^{(j)}(U(X_i)),\ i = 1, \mathbf{K}, n,\ j = 1, 2$, где $T^{(j)}(U) = \hat{v}_{j1}(u_1 - \bar{u}_1) + \ldots + \hat{v}_{jm}(u_m - \bar{u}_m)$, $\bar{u}_j = 1/U \sum_{i=1}^{n} U_i$.

Проведены численные эксперименты, иллюстрирующие применимость данного подхода для распознавания бинарных последовательностей, полученных с помощью различных генераторов (в частности, линейных регистров сдвига с различными многочленами).

Литература

1. Kharin Yu. S., Yarmola A.N. Testing of pseudo-random generators by MTD-models // Proceedings of the international security and counteracting terrorism conference. – Moscow, 2006. – P. 192–198.
2. Piatlitski A. I. The method based on binary MC(s, r) under additive distortions for estimating the model parameters of Geffe`s generator // 9th International Conference computer data analysis and modeling: complex stochastic data and systems. Vol 2. – Minsk, 2010. – P 51 – 54.
3. Кемени, Дж. Конечные цепи Маркова / Дж. Кемени, Дж. Снелл. – М. : Наука, 1970. – 272 с.
4. Харин Ю. С., Мальцев М. В. Алгоритмы статистического анализа цепей Маркова с условной глубиной памяти // Информатика, 2011, №1. – С. 34 – 43.
5. Харин, Ю. С. Математические и компьютерные основы криптологии / Ю. С. Харин, В. И. Берник, Г. В. Матвеев, С. В. Агиевич. – Мн.: Новое знание, 2003. – 381 с.

ЗАЩИТА ИНФОРМАЦИИ В КАНАЛАХ С ШУМАМИ НА ОСНОВЕ НЕ ПРИМИТИВНЫХ ЛИНЕЙНЫХ КОДОВ

Олексюк А. О., Липницкий В. А.

Военная академия Республики Беларусь, Минск, Беларусь,
e-mail: Un_ami@mail.ru

Коды Боуза-Чоудхури-Хоквингема (БЧХ-коды) нашли широчайшее применение в современных инфокоммуникационных системах. Они применены в материнских платах, используются в пейджинговой, сотовой, космической связи, в хранении данных на винчестерах, дисках. Растущий объем передачи данных ужесточает требования к применяемым помехоустойчивым кодам и к их декодирующим возможностям. Идет постоянный поиск кодов, исправляющих многократные ошибки в сочетании с эффективными декодирующими алгоритмами [1, 2]. Отмеченной проблематике и посвящен данный доклад.

В семействе БЧХ кодов наибольшей размерностью и, следовательно, наибольшей скоростью передачи информации выделяются коды C_t с проверочной матрицей $H = (b^i, b^{3i}, \ldots, b^{(2t-1)i})^T$ длиной n, где n делитель $2^m - 1$, $b = a^m$ для $m = (2^m - 1)/n$,