ЗАЩИТА ИНФОРМАЦИИ

УДК 519.2: 003.26

М.В. Мальцев, Ю.С. Харин

О ТЕСТИРОВАНИИ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ НА ОСНОВЕ ЦЕПЕЙ МАРКОВА УСЛОВНОГО ПОРЯДКА

Рассматривается цепь Маркова условного порядка, используемая для статистического тестирования криптографических генераторов. Приводятся статистические оценки параметров, доказывается состоятельность оценки порядка цепи Маркова. Показываются результаты компьютерных экспериментов для модельных и реальных данных.

Введение

Методы теории вероятностей и математической статистики широко применяются в задачах защиты информации для тестирования криптографических генераторов [1, 2]. Генератор, используемый в системах криптографической защиты информации, должен порождать выходную последовательность, неотличимую от равномерно распределенной случайной последовательности (РРСП) [1], часто называемой также «чисто случайной» последовательностью, элементы которой независимы в совокупности и имеют равномерное распределение вероятностей. Известным примером отклонения от РРСП является используемый в протоколах SSL и WEP генератор RC4 [3], в котором несколько «смещено» распределение вероятностей второго байта: вероятность получить нуль в этом байте равна 1/128, а не 1/256. Для обнаружения отклонения от модели «чистой случайности» применяется статистическое тестирование, задача которого – установить, обладает ли выходная последовательность исследуемого генератора теми или иными свойствами РРСП; к примеру, является ли распределение вероятностей байтов равномерным. Статистические тесты объединяются в так называемые батареи тестов, и для признания генератора криптостойким он должен получить положительные заключения по итогам каждого теста из батареи. Наиболее известными батареями тестов являются NIST, разработанная лабораторией информационных технологий Национального института стандартов и технологий США [4]; батарея DIEHARD [5], разработанная Джорджем Марсальей; батарея Дональда Кнута [6].

Как уже отмечалось, элементы РРСП должны быть независимыми в совокупности, однако упомянутые выше батареи тестов не позволяют определять зависимости большой глубины s, поэтому для их выявления требуются дополнительные исследования. Математической моделью, в которой распределение вероятностей будущего состояния зависит от s прошлых состояний, является цепь Маркова s-го порядка [7]. К сожалению, число независимых параметров D полносвязной цепи Маркова s-го порядка с N состояниями возрастает экспоненциально с увеличением порядка: $D = (N-1)N^s$, поэтому использовать ее напрямую для обнаружения зависимостей большой глубины в выходных последовательностях криптографических генераторов практически невозможно. Для решения этой проблемы разрабатываются так называемые «малопараметрические» модели цепи Маркова s-го порядка, которые, по существу, представляют собой частные случаи полносвязной цепи Маркова, матрица вероятностей одношаговых переходов которых может быть описана значительно меньшим числом параметров, чем D. Примерами таких моделей являются цепь Маркова с частичными связями [8] и модель Рафтери [9]. В настоящей статье для статистического тестирования применяется «малопараметрическая» модель, предложенная в [10, 11], – цепь Маркова условного порядка.

1. Цепь Маркова условного порядка

Приведем математическое описание цепи Маркова условного порядка. Примем обозначения: N – множество натуральных чисел; $A = \{0, 1, ..., N-1\}$ – пространство состояний мощности $N \in \mathrm{N}$, $2 \le N < \infty$; $J_n^m = (j_n, j_{n+1}, ..., j_m) \in A^{m-n+1}$, $m, n \in N$, $m \ge n$, – мультииндекс (цепочка $m - n + 1$ индексов); $< J_n^m > = \sum_{k=n}^{m} N^{k-n} j_k \in \{0, 1, \ldots, N^{m-n+1} - 1\}$ – числовое представление мультииндекса J_n^m; $G_k^l J_n^m$ – конкатенация мультииндексов G_k^l и J_n^m; $I\{B\}$ – индикаторная функция события B; $\{x_t \in A : t \in \mathrm{N}\}$ – однородная цепь Маркова s-го порядка ($2 \le s < \infty$) с $(s + 1)$-мерной матрицей вероятностей одношаговых переходов $P = (p_{J_1^{s+1}})$, $p_{J_1^{s+1}} = \mathrm{P}\{x_{t+s} = j_{s+1} \mid x_{t+s-1} = j_s, \ldots, x_t = j_1\}$, $J_1^{s+1} \in A^{s+1}$, $t \in \mathrm{N}$; $L \in \{1, \ldots, s-1\}$, $K = N^L - 1$ – натуральные числа; $Q^{(1)}, ..., Q^{(M)}$ – семейство M ($1 \le M \le K+1$) различных квадратных стохастических матриц порядка N: $Q^{(m)} = (q_{i,j}^{(m)})$, $0 \le q_{i,j}^{(m)} \le 1$, $\sum_{j \in A} q_{i,j}^{(m)} = 1$, $i, j \in A$, $1 \le m \le M$; $\nu_{l,y}(J_1^l) = \sum_{t=1}^{n-s} I\{x_{t+s-l-y+1} = j_1, X_{t+s-l+2}^{t+s} = J_2^l\}$, $l \ge 2$, $y \ge 0$, $l + y \le s + 1$, – частота состояния $J_1^l \in A^l$ с пропуском в y символов между j_1 и J_2^l.

Цепь Маркова s-го порядка ($2 \le s < \infty$) $\{x_t \in A : t \in \mathrm{N}\}$ называется цепью Маркова условного порядка [10, 11], если ее вероятности одношаговых переходов имеют следующий «малопараметрический» вид:

$$p_{J_1^{s+1}} = \sum_{k=0}^{K} I\{< J_{s-L+1}^s >= k\} q_{j_{b_k}, j_{s+1}}^{(m_k)}, \; J_1^{s+1} \in A^{s+1}, \tag{1}$$

где $1 \le m_k \le M \le K + 1$, $1 \le b_k \le s - L$, $0 \le k \le K$, $\min_{0 \le k \le K} b_k = 1$; при этом в последовательности $m_0, \ldots, m_K$ встречаются все элементы множества $\{1, 2, \ldots, M\}$. Последовательность L элементов J_{s-L+1}^s, определяющая условие в формуле (1), называется базовым фрагментом памяти (БФП), L – длина БФП; величина $s_k = s - b_k + 1$ называется условным порядком. Таким образом, распределение вероятностей состояния процесса в момент времени t зависит не от всех s предыдущих состояний, как это было бы для полносвязной цепи Маркова порядка s, а от $L + 1$ состояний (j_{b_k}, J_{s-L+1}^s). Число параметров модели (1) $d = 2(N^L + 1) + MN(N - 1)$. Отметим, что при $L = s - 1$, $s_0 = \ldots = s_K = s$, получаем полносвязную цепь Маркова порядка s.

Если последовательность, порождаемая криптографическим генератором, представляет собой эргодическую цепь Маркова, то с течением времени текущее распределение вероятностей стремится к стационарному распределению вероятностей. Поэтому для исследования надежности таких генераторов важно определить условия, при которых стационарное распределение вероятностей является равномерным. Следующая теорема устанавливает эти условия для цепи Маркова условного порядка.

Теорема 1 [11]. *Если цепь Маркова условного порядка (1) эргодическая, то ее стационарное распределение вероятностей является равномерным тогда и только тогда, когда*

$$\begin{cases} Q^{(m_k)} = N^{-1} \cdot \mathbf{1}_{N \times N}, \text{ если } s_k \in \{L+1, ..., s-1\}; \\ Q^{(m_k)} - \text{бистохастическая матрица, т. е. } \sum_{i \in A} Q_{ij}^{(m_k)} = 1, \forall j \in A, \text{ если } s_k = s, \end{cases}$$

где $\mathbf{1}_{N \times N}$ *–* $(N \times N)$*-матрица, все элементы которой равны 1,* $k = 0, 1, \ldots, K$.

В дальнейшем будем рассматривать случай, когда каждому значению БФП соответствует своя матрица вероятностей переходов, т. е. $m_k = k + 1$, $k = 0, 1, \ldots, K$.

Оценки максимального правдоподобия вероятностей переходов и условных порядков [10] имеют вид

$$\hat{q}_{j_0,j_{L+1}}^{(k+1)} = \begin{cases} \sum\limits_{J_1^L \in A^L} I\{< J_1^L >= k\} \dfrac{\nu_{L+2,s_k-L-1}(J_0^{L+1})}{\nu_{L+1,s_k-L-1}(J_0^L)}, & \text{если } \nu_{L+1,s_k-L-1}(J_0^L) > 0; \\ 1/N, & \text{если } \nu_{L+1,s_k-L-1}(J_0^L) = 0, \end{cases} \tag{2}$$

$$\hat{s}_k = \underset{L+1 \le y \le s}{\operatorname{argmax}} \sum_{J_1^L \in A^L} I\{< J_1^L >= k\} \sum_{j_0,\, j_{L+1} \in A} \nu_{L+2,y-L-1}(J_0^{L+1}) \ln \hat{q}_{j_0,\, j_{L+1}}^{(k+1)}, \; k = 0, \ldots, K.$$

На основе асимптотических свойств оценок (2) в [10] построен статистический тест для проверки гипотез о значении матриц вероятностей одношаговых переходов $Q^{(k)}$, $k = 1, \ldots, K+1$; $H_0 = \{Q^{(1)} = Q_0^{(1)}, \ldots, Q^{(K+1)} = Q_0^{(K+1)}\}$, $H_1 = \overline{H}_0$, где $Q_0^{(1)}$, ..., $Q_0^{(K+1)}$ – некоторые фиксированные матрицы вероятностей переходов. Если $N = 2$, $A = \{0, 1\}$ и все элементы матриц $Q_0^{(1)}, \ldots, Q_0^{(K+1)}$ равны 1/2, тест позволяет обнаруживать отклонения от РРСП и имеет следующий вид (порядок цепи Маркова, длина БФП и условные порядки предполагаются фиксированными):

$$\text{принимается решение в пользу гипотезы } \begin{cases} H_0 (PPCП): \; \rho \le \Delta, \\ H_1: \; \rho > \Delta, \end{cases} \tag{3}$$

где $\rho = \sum\limits_{J_0^{L+1} \in A^{L+1}} \sum\limits_{k=0}^{K} I\{< J_1^L >= k\} 2\nu_{L+1,s_k-L-1}(J_0^L)\left(\hat{q}_{j_0,j_{L+1}}^{(k+1)} - 1/2\right)^2$, $\Delta = G_z^{-1}(1-\alpha)$ – квантиль уровня $1 - \alpha$ ($\alpha \in (0, 1)$) стандартного χ^2-распределения с $z = 2^{L+1}$ степенями свободы.

Для оценивания длины БФП L и порядка s используется байесовский информационный критерий [12], который для цепи Маркова условного порядка принимает вид

$$(\hat{s}, \hat{L}) = \underset{2 \le s' \le S_+,\; 1 \le L' \le L_+}{\operatorname{argmin}} BIC(s', L'), \tag{4}$$

$$BIC(s', L') = -\sum_{J_0^{L'+1} \in A^{L'+2}} \sum_{k=0}^{K} I\{< J_1^{L'} >= k\} \nu_{L'+2,\, r(\hat{s}_k)}(J_0^{L'+1}) \ln \hat{q}_{j_0,\, j_{L'+1}}^{(k+1)} + 2N^{L'} \ln n,$$

где $S_+ \ge 2$, $1 \le L_+ \le S_+ - 1$ – максимально допустимые значения параметров s и L; оценки $\hat{Q}^{(k)}$ и $\hat{s}_k$ вычисляются по формуле (2).

Доказана состоятельность оценок (4):

$$\hat{s} \xrightarrow{\text{P}} s, \; \hat{L} \xrightarrow{\text{P}} L \text{ при } n \to \infty. \tag{5}$$

Теорема 2. *Если цепь Маркова условного порядка (3) стационарна, то при $n \to \infty$ оценки (4) состоятельны.*

Доказательство. Обозначим $\pi_{l,y}(J_1^l) = \mathrm{P}\{x_t = j_1, \; X_{t+y+1}^{t+y+l-1} = J_2^l\}$, $l \ge 2$, $y \ge 0$. Тогда $q_{j_0,j_{L+1}}^{(k+1)} = \dfrac{\pi_{L+2,g(s_k,L)}(J_0^{L+1})}{\pi_{L+1,g(s_k,L)}(J_0^L)}$, где $< J_1^L > = k$. Заметим, что если фрагмент $X_1^{L'} = J_1^{L'}$ фиксирован, то $-\sum\limits_{j_0,\, j_{L'} \in A} \pi_{L'+2,\,y}(J_0^{L'+1}) \ln \dfrac{\pi_{L'+2,\,y}(J_0^{L'+1})}{\pi_{L'+1,\,y}(J_0^{L'})}$ – условная энтропия $H_{J_1^{L'},\,y}\{x_{L'+1} \mid x_0\}$ $x_{L'+1}$ относительно x_0. Из асимптотических свойств оценок (2), установленных в [10, 11], следует, что выполняется сходимость по вероятности:

$$-\frac{1}{n} \sum_{J_0^{L'+1} \in A^{L'+2}} \sum_{k=0}^{K} I\{< J_1^{L'} >= k\} \nu_{L'+2,\, g(\hat{s}_k, L')}(J_0^{L'+1}) \ln \frac{\nu_{L'+2,\, g(\hat{s}_k, L')}^{s'}(J_0^{L'+1})}{\nu_{L'+1,\, g(\hat{s}_k, L')}(J_0^{L'})} \xrightarrow{\text{P}}$$

$$\xrightarrow{\text{P}} \sum_{J_1^{L'} \in A^{L'+2}} \sum_{k=0}^{K} I\{< J_1^{L'} >= k\} I\{< J_1^{L'} >= k\} H_{J_1^{L'},\, g(y_k,\, L')}\{x_{L'+1} \mid x_0\},\ L' + 1 \le y_k \le s'.$$

Используя свойства энтропии и методы, описанные в статье (12), приходим к требуемому результату (5), показав, что $\text{P}\{(\hat{s}, \hat{L}) \in ([2, s_+] \times [1, L_+]) \setminus (s, L)\} \xrightarrow{\text{P}} 0$ при $n \to \infty$. ■

2. Обобщения модели цепи Маркова условного порядка

Обобщения модели (1) возможны по двум направлениям:
– использование обобщенного базового фрагмента памяти;
– использование многомерных матриц $Q^{(1)}, ..., Q^{(M)}$.

Дадим краткое описание этих обобщений. Обозначим: $W = \{1, \ldots, s\}$; $W_L = \{v_1, \ldots, v_L\}$, $v_1, \ldots, v_L \in W$, $v_i \ne v_j$ при $i \ne j$; $\overline{W} = W \setminus W_L$.

Цепь Маркова s-го порядка $\{x_t \in A : t \in \text{N}\}$ назовем цепью Маркова условного порядка с обобщенным базовым фрагментом памяти W_L, если ее вероятности одношаговых переходов имеют вид

$$p_{J_1^{s+1}} = \sum_{k=0}^{K} I(< S(J_1^s, W_L) >= k) q^{(m_k)}_{j_{b_k}, j_{s+1}}, \tag{6}$$

где S – функция-селектор, $S(J_1^s, W_L) = (j_{v_1}, \ldots, j_{v_L})$. Если $W_L = \{s - L + 1, \ldots, s\}$, то (6) преобразуется в (1) и в этом частном случае приходим к введенной ранее модели.

В рамках второго направления обобщения модели цепи Маркова условного порядка соотношение (1) имеет следующий вид:

$$p_{J_1^{s+1}} = \sum_{k=0}^{K} I(< J_{s-L+1}^{s} >= k) q^{(m_k)}_{j_{b_k^{(1)}}, \ldots j_{b_k^{(r)}}, j_{s+1}}, \tag{7}$$

где $Q^{(m_k)} = (q^{(m_k)}_{j_{b_k^{(1)}}, \ldots j_{b_k^{(r)}}, j_{s+1}})$ – $(r + 1)$-мерная матрица вероятностей одношаговых переходов, $1 \le r \le s–L$; $\{b_k^{(1)}, \ldots, b_k^{(r)}\} \subseteq \{1, \ldots, s - L\}$ – множество r различных элементов. Если $r = 1$, то (7) преобразуется в исходную модель (1).

3. Численные результаты

3.1. Модельные данные

Генерировались $U = 1000$ реализаций цепи Маркова условного порядка длительности $n = 100\,000$ с параметрами $N = 2$, $A = \{0, 1\}$, $s = 16$, $L = 4$, $(s_0, \ldots, s_K) = (6, 16, 8, 14, 15, 10, 5, 12, 11, 7, 16, 13, 7, 16, 9, 8)$. В ходе экспериментов вычислялась доля решений в пользу H_1:

$$\hat{\alpha} = \frac{1}{U} \sum_{u=1}^{U} I\{\rho_u > \Delta\},$$

где ρ_u – значение статистики ρ, вычисленной по u-й реализации. При вычислении ρ_u все значения параметров модели (за исключением матриц вероятностей одношаговых переходов) полагались априорно известными. На рис. 1 по горизонтальной оси откладывался номер реализации, по вертикальной – значение тестовой статистики ρ; точками отмечались величины ρ_u, сплошной линией изображен порог теста $\Delta = G_{32}^{-1}(0{,}95) \approx 46{,}2$.

В левой части рис. 1 представлены результаты экспериментов при верной гипотезе H_0, когда все элементы матриц вероятностей одношаговых переходов равны $1/N = 1/2$. Значение $\hat{\alpha} = 0{,}045$, вычисленное в ходе эксперимента, согласуется с теоретическими результатами. В правой части рис. 1 представлены результаты экспериментов для истинной альтернативы H_1. В этом случае матрицы вероятностей одношаговых переходов генерировались случайным образом так, чтобы $|q_{ij}^{(k)} - 0{,}5| \le 0{,}01$, $k = 1, \ldots, K+1$, $i, j \in A$.

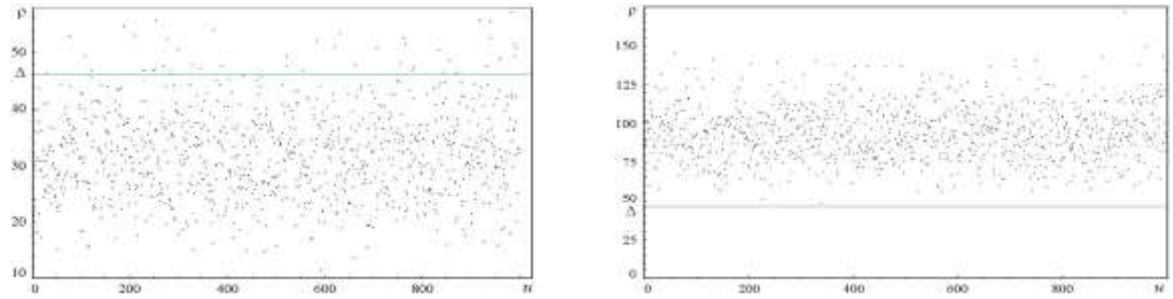

Рис. 1. Результаты для модельных данных

3.2. Реальные данные

Исследовались выходные последовательности самосжимающего генератора [13] и регистра сдвига с переменной обратной связью [14]. Характеристический многочлен самосжимающего генератора имеет вид $f(x) = x^{36} + x^{11} + 1$ (период выходной последовательности $T_1 = 2^{18}$), характеристические многочлены регистра сдвига с переменной обратной связью – $f_1(x) = x^{23} + x^5 + 1$, $f_2(x) = x^{23} + x^9 + 1$, управляющий многочлен – $g(x) = x^{17} + x^{16} + x^{12} + x^4 + 1$ (период выходной последовательности $T_2 \geq 2^{17} - 1$). Все вышеперечисленные многочлены являются примитивными. Генерировалось по $U = 1000$ реализаций выходной последовательности каждого генератора длительности $n = 100\,000$ со случайно выбранным начальным заполнением регистров сдвига с линейной обратной связью, входящих в исследуемые генераторы. При фиксированной длине БФП L изменялся порядок цепи Маркова s от L+1 до 100. При этом первая половина последовательности длины $n_{0,5} = 50\,000$ использовалась для построения оценок условных порядков по формуле (2), вторая половина – для вычисления тестовой статистики ρ. Отметим, что распределение вероятностей тестовой статистики, для вычисления которой использовались оценки ($\hat{b}_0$, …, $\hat{b}_K$), построенные по всей реализации длительности n, отличается от χ^2-распределения с z степенями свободы (рис. 2). Сплошной линией изображен график функции χ^2-распределения вероятностей с $z = 32$ степенями свободы, точками изображена выборочная функция распределения. В левой части рис. 2 представлены результаты для случая, когда оценивание производится по первой половине реализации, в правой – для случая, когда оценивание производится по всей реализации. Таким образом, целесообразно оценивание $\{b_k\}$ проводить по первой половине наблюдаемой реализации выходной последовательности. Такой подход и использовался далее при тестировании двух указанных выше криптографических генераторов.

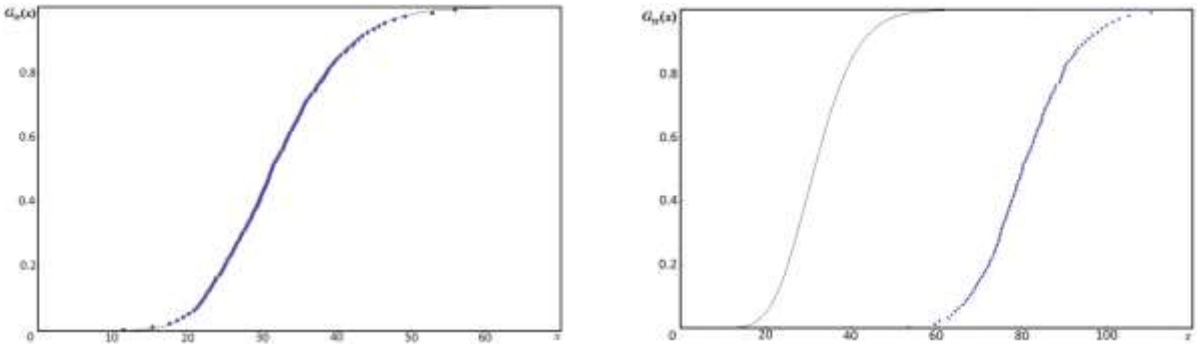

Рис. 2. Функции распределения и их оценки

Для каждой пары (s, L) вычислялась величина $\hat{\alpha}$, которая отмечалась на рис. 3 и 4 точкой (по горизонтальной оси откладывался порядок s). Сплошная линия на рисунках – уровень значимости α (рис. 3 и 4).

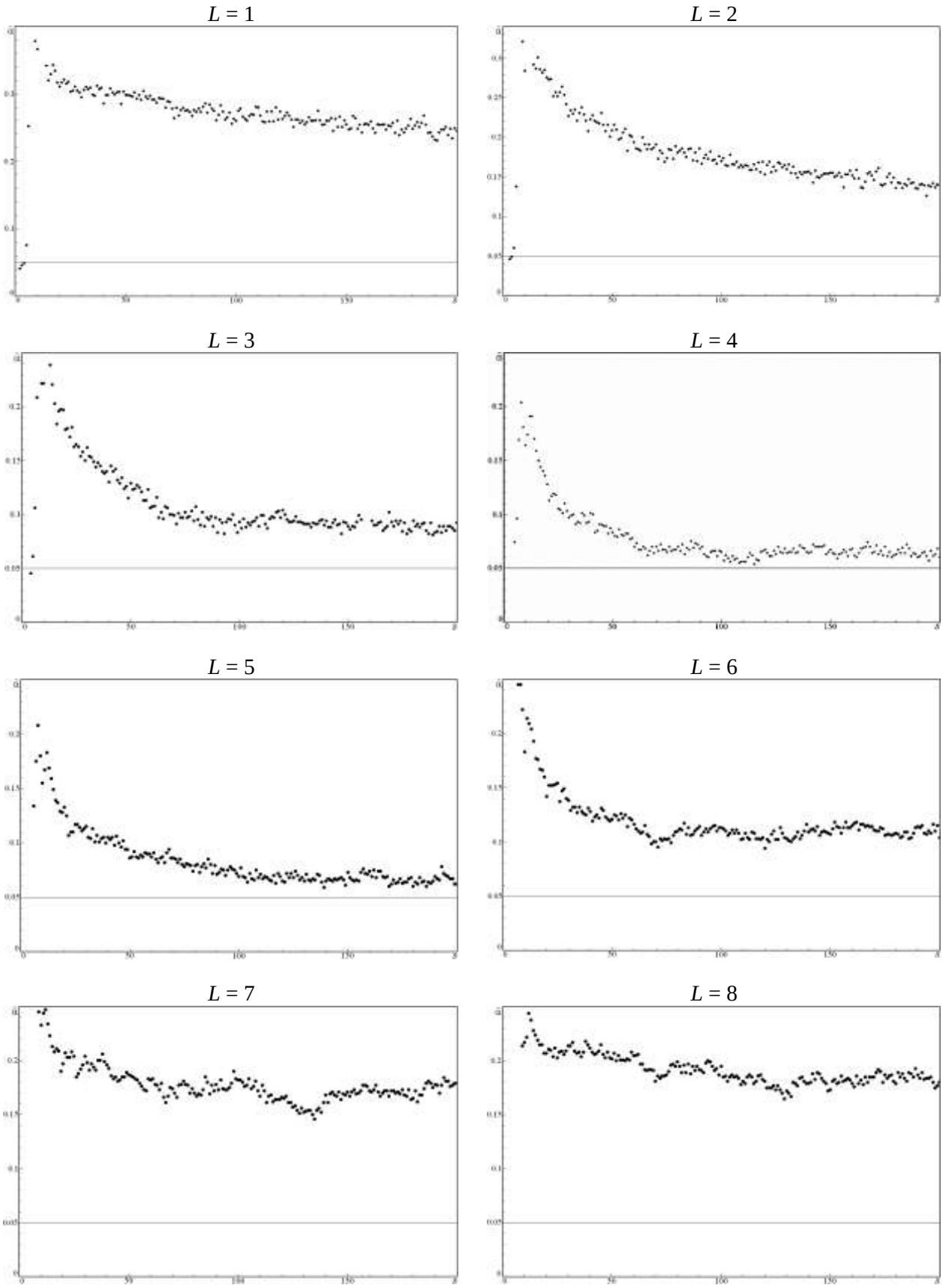

Рис 3. Результаты для самосжимающего генератора при $L \in \{1,\ldots,8\}$

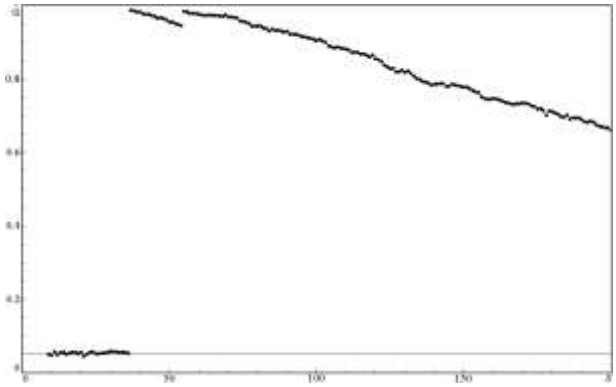

Рис. 4. Результаты для регистра сдвига с переменной обратной связью при $L = 8$

Для регистра сдвига с переменной обратной связью (см. рис. 4) доля отклонений гипотезы H_0 заметно выше, чем для самосжимающего генератора (см. рис. 3); при $s \leq 36$ значение $\hat{\alpha}$ не превышает 0,057, но затем при $s = 37$ резко возрастает до 0,988, уменьшаясь далее с ростом s (еще один небольшой «скачок» наблюдается при $s = 55$).

Таким образом, результаты компьютерных экспериментов демонстрируют применимость теста (3) при увеличении параметра L. Отметим нелинейный характер зависимости $\hat{\alpha}$ как от порядка s, так и от длины БФП L. К примеру, для самосжимающего генератора при $s = 3$ число решений в пользу H_1 больше, чем при $s = 4$, а при $L = 6$ число решений в пользу H_1 наибольшее при $L < 50$.

Заключение

В статье предложен подход к статистическому обнаружению отклонений выходных последовательностей криптографических генераторов от модели «чисто случайной» последовательности. Для обнаружения отклонений использовалась цепь Маркова условного порядка – математическая модель, учитывающая зависимости высоких порядков при относительно небольшом числе независимых параметров. Доказана состоятельность статистических оценок порядка и длины базового фрагмента памяти. Теоретические результаты проиллюстрированы на модельных данных и на выходных последовательностях самосжимающего генератора и регистра сдвига с переменной обратной связью.

Список литературы

1. Математические и компьютерные основы криптологии / Ю.С. Харин [и. др.]. – Минск : Новое знание, 2003. – 382 с.

2. Максимов, Ю.И. О цепях Маркова, связанных с двоичными регистрами сдвига со случайными элементами / Ю.И. Максимов // Труды по дискретной математике. – 1997. – Т. 1. – С. 203–220.

3. Sepehrdad, P. Discovery and Exploitation of New Biases in RC4 / P. Sepehrdad, S. Vaudenay, M. Vuagnoux // Lecture Notes in Computer Science. – 2011. – Vol. 6544. – P. 74–91.

4. A statistical test suite for random and pseudorandom number generators for cryptographic applications / A. Rukhin [et al.] // National Institute of Standards and Technology [Electronic resource]. – USA, 2010. – Mode of access : http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf. – Date of access : 17.04.2013.

5. Marsaglia, G. The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness / G. Marsaglia [Electronic resource]. – Florida State University, 1995. – Mode of access : http://www.stat.fsu.edu/pub/diehard/. – Date of access : 01.06.2013.

6. Кнут, Д.Э. Искусство программирования: в 3 т. Т. 1: Получисленные методы / Д. Э. Кнут. – М. : Вильямс, 2007. – 832 с.

7. Doob, J.L. Stochastic processes / J.L. Doob. – N. Y. : Wiley, 1953. – 654 p.

8. Харин, Ю.С. Цепь Маркова с частичными связями ЦМ(*s*, *r*) и статистические выводы о ее параметрах / Ю.С. Харин, А.И. Петлицкий // Дискретная математика. – 2007. – Т. 19, № 2. – С. 109–130.

9. Raftery, A.E. A model for high-order Markov chains / A.E. Raftery // J. Royal Statistical Society. – 1985. – Vol. B-47, № 3. – P. 528–539.

10. Харин, Ю.С. Статистическая проверка гипотез о параметрах цепи Маркова условного порядка / Ю.С. Харин, М.В. Мальцев // Весці НАН Беларуси. Сер. фіз.-мат. навук. – 2012. – № 3. – С. 5–12.

11. Мальцев, М.В. Об асимптотических свойствах статистических оценок параметров цепи Маркова условного порядка / М.В. Мальцев, Ю.С. Харин // Весці НАН Беларуси. Сер. фіз.-мат. навук. – 2013. – №1. – С. 5–12.

12. Csiszar, I. Consistency of the BIC order estimator / I. Csiszar, P. Shields // Electronic research announcments of the American mathematical society. – 1999. – Vol. 5. – P. 123–127.

13. Meier, W. The self-shrinking generator / W. Meier, O. Staffelbach // Advances in Cryptology – EUROCRYPT 94. – Springer-Verlag, 1995. – P. 205–214.

14. Основы криптографии / А.П. Алферов [и др.]. – М. : Гелиос АРВ, 2001. – 480 с.

Поступила 11.06.2013

НИИ прикладных проблем математики
и информатики БГУ,
Минск, пр. Независимости, 4
e-mail: kharin@bsu.by, maltsew@mail.ru

M.V. Maltsev, Yu.S. Kharin

ON TESTING OF CRYPTOGRAPHYC GENERATORS OUTPUT SEQUENCES USING MARKOV CHAINS OF CONDITIONAL ORDER

The paper deals with the Markov chain of conditional order, which is used for statistical testing of cryptographic generators. Statistical estimations of model parameters are given. Consistency of the order estimator is proved. Results of computer experiments are presented.