Литература

1. Method for protecting speech information / H. V. Davydau, V. A. Papou, A. V. Patapovich [et al.]. – Doklady BSUIR, No.8(94), 2015, P. 107–110.

2. Seitkulov Y. Rationale for the method of formation of the combined speech masking signals / Y. Seitkulov, S. Boranbayev, B. Yergalieva, G. Davydov, A. Patapovich // 2014 IEEE 8th International Conference on Application on Information and Communication Technologies (AICT), Astana, Kazakhstan.

3. Давыдов, Г. В. Синтез речеподобных сигналов на белорусском языке / Г. В. Давыдов, В. А. Попов, А. В. Потапович, Е. Н. Сейткулов, И. В. Савченко / Доклады БГУИР. – 2015. – № 4 (90). – С. 27–32.

УДК 003.26+519.2

О ПРИМЕНЕНИИ ДИНАМИЧЕСКОГО ТЕСТА МНОГОМЕРНОЙ ДИСКРЕТНОЙ РАВНОМЕРНОСТИ ДЛЯ ОЦЕНКИ КАЧЕСТВА СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

А. Н. ГАЙДУК, М. В. МАЛЬЦЕВ

Учреждение Белорусского государственного университета «Научно-исследовательский институт прикладных проблем математики и информатики», г. Минск, Республика Беларусь

Введение

Надежные системы криптографической защиты информации невозможны без использования стойких генераторов случайных числовых последовательностей (ГСЧП). ГСЧП необходимы для выработки ключей, векторов инициализации, стартовых значений переменных в алгоритмах и для других задач. Двоичные выходные последовательности, которые выдает стойкий ГСЧП, должны быть неотличимы от «чистой случайности» – последовательности независимых испытаний Бернулли с вероятностью успеха 1/2. Для оценки стойкости ГСЧП используются батареи (наборы) статистических тестов, задача которых – выявление всевозможных типов отклонений от «чистой случайности». На практике широко используются такие батареи тестов как NIST, Diehard, TestU01. Однако эти и другие батареи тестов обладают рядом недостатков и ограничений: они проверяют простую нулевую гипотезу, не фиксируют семейство альтернатив, могут не обнаруживать сравнительно простые зависимости. Например, в работе [1] генератор, построенный на основе комбинации двух регистров сдвига со следующими примитивными многочленами:

$$f(x) = x^{32} + x^{30} + x^{29} + x^{26} + x^{24} + x^{22} + x^{21} + x^{18} + x^{16} + x^{14} + x^{13} + x^{10} + x^{8} + x^{6} + x^{5} + x^{2} + 1,$$

$$g(x) = x^{27} + x^{5} + x^{2} + x + 1$$

успешно прошел все тесты батареи NIST. В работе [2] показано, что батарея NIST может не отбраковывать криптографически слабые двоичные последовательности, содержащие повторяющиеся блоки большой длины. Приведенные примеры показывают, что актуальной задачей является разработка новых методов и алгоритмов анализа стойкости генераторов случайных и псевдослучайных числовых последовательностей.

1. Оценка многомерной дискретной равномерности случайных последовательностей

Проблема оценки многомерной дискретной равномерности является одной из важнейших задач анализа качества ГСЧП. Один из традиционно используемых для решения этой задачи тестов – тест многомерной дискретной равномерности по непересекающимся фрагментам длины s – s-граммам (далее – МДРН(s)-тест) заключается в том, чтобы определить выполняется ли гипотеза согласия наблюдаемой последовательности s-грамм с s-мерным дискретным равномерным распределением. Данный тест, основанный на анализе частот появления s-грамм в двоичной последовательности направлен на проверку глобальной равномерности, однако глобальные частотные тесты обладают ограниченной чувствительностью к локальным нарушениям структуры, включая временные корреляции, квазипериодичность и другие виды зависимостей, не приводящих к значимому отклонению глобального распределения. В связи с этим в настоящей работе предлагается метод статистического тестирования, основанный на распределении длины минимальных подпоследовательностей, содержащих фиксированное число вхождений заданной s-граммы. Данный метод развивает предложенный в работе [3] подход динамического разбиения тестируемой последовательности.

2. Распределение вероятностей тестовой статистики

Обозначим: $\{X_i : i \in \mathbb{N}\}$ – случайная последовательность, где каждый элемент X_i принадлежит множеству $\{0, 1\}$, G_j – s-грамма:

$$G_j = (X_j, X_{j+1}, ..., X_{j+s-1}),\ j = 1, 2, ..., N - s + 1,\ s \geq 1\,.$$

Пусть $ã \in \{0,1\}^s$ – некоторое фиксированное значение s-граммы. В предположении истинности нулевой гипотезы H_0 о независимости и равномерной распределенности случайных величин X_i вероятность того, что s-грамма G_j равна $ã$, имеет вид:

$$\mathrm{P}\{G_j = \gamma\} = \frac{1}{2^s}\,.$$

Определим случайную величину K_w как минимальную длину подпоследовательности s-грамм, содержащую w появлений $ã$:

$$K_w = \min\left\{ k \in \mathbb{N} \,\middle|\, \sum_{j=1}^{k} 1\{G_j = \gamma\} = w \right\},$$

где $1\{A\}$ – индикаторная функция события A: $1\{A\} = 1$, если A наступает, $1\{A\} = 0$ в противном случае.

При верной гипотезе H_0, величина K_w имеет отрицательное биномиальное распределение с параметрами w и $p = \dfrac{1}{2^s}$:

$$\mathrm{P}_w(k)=\mathrm{P}\{K_w=k\}=C_{k-1}^{w-1}\cdot\frac{1}{2^{ws}}\left(1-\frac{1}{2^s}\right)^{k-w},k\geq w$$

Таким образом, для заданного *w*, по выборке значений $K_w^{(1)},...,K_w^{(M)}$, полученных из последовательности $X_1,...,X_N$, можно эмпирически оценить распределение длины K_w и сравнить его с теоретическим, соответствующим гипотезе H_0.

3. Алгоритм динамического МДРН(*s*)-теста

На основании представленных выше результатов сформулируем алгоритм тестирования двоичной последовательности с использованием динамического МДРН(*s*)-теста

1. Фиксируется *s*-грамма $\tilde{a}\in\{0,1\}^s$ и число вхождений *w*.

2. Определяется длина подпоследовательности $K_w^{(i)}$, необходимая для достижения *w* вхождений *s*-граммы $\tilde{a}$ в данную подпоследовательность. Данная подпоследовательность удаляется и процесс повторяется.

3. Полученное эмпирическое распределение $\{K_w^{(i)}\}$ сравнивается с теоретическим $\mathrm{P}_w(k)$ с помощью критерия согласия $\div^2$.

4. В случае статистически значимого отклонения делается вывод о нарушении гипотезы равномерности и/или независимости.

В таблицах 1–4 представлены границы интервалов Δ_- и Δ_+ и вероятности попадания K_w в эти интервалы – P_Δ для различных параметров динамического теста многомерной дискретной равномерности. Для *s*=1 результаты представлены в работе [4].

Таблица 1 – Вероятности интервалов для *w* = 16, *s* = 2

$[\Delta_-, \Delta_+]$	16–48	49–54	55–58	59–62	63–66	67–72	73–79	≥80
P_Δ	0,123178	0,136602	0,112476	0,117900	0,113102	0,144557	0,118760	0,133425

Таблица 2 – Вероятности интервалов для *w* = 16, *s* = 3

$[\Delta_-, \Delta_+]$	16–94	95–106	107–116	117–125	126–135	136–147	148–163	≥164
P_Δ	0,123153	0,124609	0,129413	0,122702	0,128939	0,129722	0,119895	0,121567

Таблица 3 – Вероятности интервалов для *w* = 16, *s* = 4

$[\Delta_-, \Delta_+]$	16–187	188–212	213–232	233–251	252–271	272–295	296–328	≥329
P_Δ	0,126696	0,126944	0,125495	0,125080	0,124395	0,125929	0,121153	0,124308

Таблица 4 – Вероятности интервалов для *w* = 16, *s* = 5

$[\Delta_-, \Delta_+]$	16–371	372–422	423–463	464–502	503–542	543–590	591–695	≥660
P_Δ	0,124184	0,126390	0,126220	0,126283	0,122603	0,124747	0,125406	0,124167

Заключение

В данной работе предложен статистический тест для проверки гипотезы о дискретной многомерной равномерности, основанный на анализе распределения длины минимальных подпоследовательностей, содержащих фиксированное число вхождений заданной s-граммы. В отличие от классического теста МДРН, оценивающего глобальные характеристики распределения s-грамм, предложенный подход позволяет выявлять локальные отклонения от равномерности и независимости. Преимуществом данного подхода является чувствительность к неравномерностям, существенно не влияющим на глобальную частоту появления s-грамм, но нарушающим структуру независимости и однородности. Рассчитаны теоретические вероятности попадания случайной величины K_w в заданный интервал, что позволяет на практике задать конкретные области принятия и отклонения нулевой гипотезы.

Литература

1. Zubkov, A. M. Testing the NIST Statistical Test Suite on artificial pseudorandom sequences / A. M. Zubkov, A. A. Serov // Математические вопросы криптографии. – 2019. – № 10:2. – С. 89–96.
2. Zubkov, A. M. Experimental study of NIST Statistical Test Suite ability to detect long repetitions in binary sequences / A. M. Zubkov, A. A. Serov // Математические вопросы криптографии. – 2023. – № 14:2. – С. 137–145.
3. Akcengiz, Z. Statistical Randomness Tests of Long Sequences by Dynamic Partitioning / Z. Akcengiz [et al.] // 2020 International Conference on Information Security and Cryptology (ISCTURKEY), Ankara, Turkey. – 2020. – P. 68–74.
4. Гайдук, А. Н. О применении динамического теста монобит для статистического тестирования случайных и псевдослучайных последовательностей / XIV Белорусская математическая конференция: материалы Международной научной конференции, Минск, 28 октября – 1 ноября 2024 г. В трех частях. Часть 3. – Минск: Беларуская навука, 2024. – С. 124.