Koreneva A.M., Fomichev V.M.

Statistical testing of pseudorandom sequences

Key words: algorithms, ideal random sequence, cryptography, pseudo-random sequence, statistical testing.

The article systematizes the basic scientific principles about statistical testing of random and pseudo-random sequences that are widely used in cryptographic systems for keys generation or forming some additional information (random numbers, initialization vectors and so on). The article includes a brief review of the known approaches to randomness testing and statistical test suites developed in the last decades. We point out that the perspective research area could be statistical testing multidimensional arrays.

А.М. Коренева, В.М. Фомичёв

СТАТИСТИЧЕСКОЕ ТЕСТИРОВАНИЕ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Введение

Категории необходимости и случайности образуют в философии пару противоположных и взаимодополняющих фундаментальных категорий. В процессе человеческого познания окружающего мира обнаруживается, на первый взгляд, явная корреляция данной пары категорий с другой фундаментальной парой категорий: знание и незнание. Однако, оснований для отождествления случайности с незнанием оказывается не так уж много. Более того, развитие науки уже в XX веке показало, что цепь случайных поистине непредсказуемых событий приводит исследователя не к хаосу, а к весьма жестким закономерным выводам глобального характера. Этот тезис нетрудно проиллюстрировать с помощью центральной предельной теоремы (и других теорем) теории вероятностей. Случайность стала предметом исследования во многих науках: в математических дисциплинах – в математической статистике, в теории игр, теории нечетких множеств, в физике и химии – при изучении свойств микромира, в экономике – при исследовании влияния случайных факторов на зарождение и развитие экономических кризисов, на траектории курсов мировых валют, в истории и социологии – при исследовании значения фактора случайности на развитие исторических событий и на смену эпох.

Отметим особенность систем случайных объектов, которая может показаться в определенном смысле парадоксальной. Гораздо чаще можно описать, в крайнем случае, предсказать, глобальные, нежели локальные закономерности больших систем. Это обуславливает два безусловно востребованных современных направления исследования: поиск глобальных закономерностей случайных систем и обоснование для случайной системы непредсказуемости событий локального характера.

Данная статья посвящена систематизации современных знаний о случайных последовательностях элементов заданного множества (как правило, чисел) и об источниках таких последовательностей. Случайные последовательности чисел или элементов других множеств используются во многих областях науки, в частности, для экспериментального исследования свойств сложных объектов и систем. Наш интерес к случайным последовательностям связан, прежде всего, с приложениями их свойств в криптографии.

Случайные последовательности. **Случайные последовательности** (СП) играют в криптографии важную роль, они используются для формирования ключевых и инициальных параметров криптографических алгоритмов и протоколов, в том числе, последовательностей шифрующих подстановок в поточных криптосистемах. Случайность

и криптография тесно взаимосвязаны: основная цель криптографических систем состоит в преобразовании неслучайных осмысленных открытых текстов в псевдослучайную (кажущуюся случайной) последовательность символов шифрованного текста. Это свойство криптосистем используют для генерации **псевдослучайных последовательностей** (ПСП).

Существуют различные подходы к формальному определению термина «случайность», основанные на понятиях вычислимости и алгоритмической сложности [1].

Наилучшие криптографические свойства криптосистемы достигаются при использовании так называемых **идеальных случайных последовательностей** (ИСП), математическая модель которых представляется реализацией последовательности независимых случайных величин, имеющих равномерное распределение вероятностей на заданном конечном алфавите. Такие последовательности называют также **равномерно распределёнными** (на некотором конечном множестве) **случайными последовательностями** (РРСП). Описанию свойств РРСП посвящено множество работ, в частности, [2-4].

РРСП (на множестве X мощности k) – это последовательность $\{\zeta_1,\ldots,\zeta_t,\ldots\}$ с.в., принимающих значения из множества X, определённых на некотором вероятностном пространстве и удовлетворяющих двум базовым условиям при любом $n \in N$:

1) для любых номеров $1 \le t_1 < \ldots < t_n$ с.в. $\zeta_{t_1},\ldots,\zeta_{t_n}$ независимы в совокупности;

2) с.в. ζ_n равномерно распределена на X, то есть $P(\zeta_t = x) = 1/k$ для любого $x \in X$.

При базовых условиях выполнено для любых номеров $1 \le t_1 < \ldots < t_n$:

1) распределение n–мерной с.в. $(\zeta_{t_1},\ldots,\zeta_{t_n})$ является равномерным на множестве X^n;

2) последовательность $\zeta_{t_1},\ldots,\zeta_{t_n},\ldots$ есть РРСП (воспроизводится при «прореживании»);

3) (воспроизводится при суммировании), то есть для неслучайной/случайной последовательности $\{\eta_t\}$ над аддитивной группой X, не зависящей от $\{\zeta_t\}$, СП $\{\zeta_t + \eta_t\}$ есть РРСП;

4) предсказание значения ζ_n при известных знаках $\zeta_1,\ldots,\zeta_{n-1}$ невозможно, то есть для любого набора $(x_1,\ldots,x_n) \in X^n$ выполнено: $P(\zeta_n = x_n / \zeta_1 = x_1,\ldots,\zeta_{n-1} = x_{n-1}) = P(\zeta_n = x) = 1/k$ (при анализе рассматривают также предсказуемость предыдущих значений по промежуточному отрезку последовательности).

Цель и задачи статистического тестирования ПСП. Тестирование ПСП на случайность – это способ распознавания ее определенных закономерностей с помощью сравнения характеристик ПСП с аналогичными характеристиками ИСП.

С помощью статистического тестирования ПСП решаются следующие задачи:

1)оценка свойств выходной последовательности генератора ПСП с точки зрения использования в криптографическом алгоритме (например, в качестве секретного ключа);

2)оценка качества криптографических примитивов (хеш-функций, блочных и поточных шифров) по их выходным последовательностям, от которых требуется неотличимость от ИСП, в частности, проверка таких криптографических свойств, как лавинный эффект изменения выходных данных алгоритмов при искажениях элементов входных данных, корреляция промежуточных и выходных последовательностей;

3)идентификация генераторов ПСП, выдающих «неслучайные» последовательности; разработка новых генераторов ПСП; проверка корректности реализации генераторов ПСП.

Суть тестирования обычно сводится к проверке так называемой «нулевой гипотезы» H_0 относительно исследуемой последовательности $x^l=(x_1,\ldots,x_l)$ длины l, согласно которой x^l получена на основе l независимых испытаний вероятностной схемы с равномерным распределением. Вообще статистический тест T есть двузначная функция T: $A^*\rightarrow\{$принять, отвергнуть$\}$, где A^* – множество последовательностей в алфавите A. Статистический тест T разделяет множество V_l последовательностей длины l на множество $V_{l,0}$ «неслучайных» последовательностей (как правило, относительно небольшое) и множество $V_{l,1}=V_l\backslash V_{l,0}$ случайных последовательностей. Вероятность ρ того, что тест отвергает случайно выбранную двоичную последовательность x^l, равна $|V_{l,0}|/2^l$. Как правило, в реальных тестах ρ≤0,01.

Сложность точного вычисления функции T велика ввиду громоздкости области определения. Поэтому статистическое тестирование для принятия/отклонения гипотезы H_0 выполняется с помощью статистики f_T, то есть относительно просто вычислимой функции, отображающей множество последовательностей во множество действительных чисел, и вероятностного распределения статистики для гипотезы H_0, определяемого теоретико-вероятностными методами. Статистический тест – это совокупность статистики, вычисленной по исходным данным, и решающего правила, в соответствии с которым по значению статистики определяют, принять или отклонить гипотезу H_0.

Статистический тест является вероятностным, в силу этого возникают ошибки двух родов, являющиеся важными характеристиками теста:

1) *ошибка* α *первого рода*, если последовательность случайна, но H_0 отклоняется;

2) *ошибка* β *второго рода*: если последовательность не случайна, но H_0 принимается.

Решение о прохождении последовательностью статистического теста принимается на основе критериев трех типов: на основе порогового значения, на основе доверительного интервала, на основе вычисления *p*-значения (*p-value*).

Подход на основе порогового значения связан со сравнением вычисленной для тестируемой последовательности x^l длины l статистики теста $f(x^l)$ с некоторым пороговым значением $c(l)$. Последовательность x^l не проходит статистический тест (гипотеза H_0 отклоняется), если $f(x^l)>c(l)$. Данный подход не считается достаточно надежным.

При подходе на основе доверительного интервала последовательность x^l не проходит статистический тест, если $f_T(x^l)$ находится вне пределов доверительного интервала значений статистики, вычисленного для заданного уровня значимости α. Данный критерий более надежный по сравнению с первым.

Третий класс критериев опирается на вычисление характеристики теста из интервала (0,1), называемой *p-значением* (*p-value*). Строение статистики теста, рассматриваемой как случайная величина с известным законом распределения, таково, что большие значения указывают на некий дефект случайности последовательности. В предположении случайности последовательности *p-value* есть вероятность того, статистика теста примет значение большее, чем наблюдаемое при опыте. То есть малые значения *p-value* соответствуют неслучайности последовательности. Решающее правило таково: при уровне значимости α последовательность x^l не проходит статистический тест, если *p-value*<α. Значения α рекомендуется брать из интервала [0,001, 0,01].

Преимущество данного подхода по сравнению с предыдущими в том, что единожды рассчитанную вероятность *p-value* сравнивают с произвольно выбранным уровнем значимости α без дополнительных расчетов.

Таким образом, основные этапы тестирования ПСП таковы:

- формулировка гипотезы H_0 о случайности последовательности;
- задание уровня значимости α (вероятности ошибки 1-го рода), обычно $\alpha\in[10^{-3};10^{-2}]$;

- вычисление значения статистики $f_т(x^l)$ для исследуемой последовательности x^l;
- вычисление $p\text{-}value \in (0;1)$ по формуле, зависящей от конкретного теста;
- сравнение *p-value* с α: если *p-value* >α, то тест на случайность пройден успешно.

Существующие инструменты для статистического тестирования ПСП. Для выявления закономерностей к анализируемым ПСП (или к их отрезкам различной длины) применяют широкий спектр различных статистических тестов, разработанных в последние десятилетия. Приведем известные наборы статистических тестов:

1. 11 тестов: Donald Knuth (Stanford University), The Art Of Computer Programming Vol. 2 Seminumerical Algorithms;
2. 15 тестов: Andrew Rukhin, et. al. (NIST ITL), NIST Statistical Test Suite;
3. 12 тестов: George Marsaglia (Florida State University), DIEHARD;
4. 11 тестов: Pierre L'Ecuyer, Richard Simard (Departement d'Informatique et de Recherche Operationnelle Universite de Montreal), TestU01;
5. 5 тестов: Helen Gustafson, et. al. (Queensland University of Technology), Crypt-XS.

Существуют другие описания и реализации статистических тестов, во многом повторяющие тесты из представленных выше наборов:

1. Alfred Menezes и др., Handbook of Applied Cryptography;
2. Peter Hellekalek (University of Salzburg), The pLab Project;
3. John Walker (Autodesk, Inc.), ENT;
4. Robert G. Brown (Duke University), Dieharder;
5. George Marsaglia (Florida State University), Wai Wan Tsang (The University of Hong Kong), «Distilled» version of Diehard.

Несмотря на немалое количество существующих реализаций статистических тестов ПСП, данное направление постоянно развивается, и в настоящее время активно появляются новые проекты, которые предлагают новые реализации рассмотренных тестов, в том числе, в условиях распределенных вычислительных систем.

Рассмотренные наборы статистических тестов ПСП составляют удобный и гибкий инструмент исследования генераторов ПСП, применяемых в криптографических приложениях.

Пакет NIST STS обладает большей гибкостью, расширяемостью и эффективностью (с точки зрения временных затрат на осуществление тестирования) и является наиболее полным из имеющихся пакетов для статистического тестирования двоичных последовательностей (подробнее можно посмотреть в работах [5-7]). На основе пакета NIST STS могут быть построены методики более полного статистического и структурного анализа последовательностей, учитывая то, что для надежной оценки качества ПСП, выработанной генератором, целесообразно проводить не одно, а несколько испытаний.

Все тесты направлены на выявление различных дефектов случайности. На практике принятие или отвержение нулевой гипотезы основывают на результатах применения нескольких независимых тестов. Когда независимые тесты приводят к различным выводам, используется комбинирование результатов тестов с помощью статистик, учитывающих совокупность результатов всех использованных тестов. При небольшом количестве комбинируемых тестов используется статистика Фишера-Пирсона, которая сравнивается с распределением *хи-квадрат*. Если количество комбинируемых тестов велико, то рекомендуется применение теста Колмогорова-Смирнова.

В таблице 1 даны некоторые тесты для тестирования ПСП различных длин.

Таблица 1. – *Статистические тесты для ПСП различных длин*

№	Пакеты стат. тестов	Тестирование ПСП длины до 300 бит	Тестирование ПСП длины порядка 10^6 бит
1.	Тесты Д. Кнута	-	• критерий частот • критерий серий • критерий «максимум-t» • критерий монотонности
2.	NIST STS	• частотный побитовый тест (Frequency Test) • частотный блочный тест (Frequency Test within a Block) • тест на серию одинаковых бит (Runs Test) • тест на совпадение неперекрывающихся шаблонов (Non-overlapping Template Matching Test) • тест на периодичность (Serial Test) • тест рангов бинарных матриц (Binary Matrix Rank Test) • тест приблизительной энтропии (Approximate Entropy Test) • тест кумулятивных сумм (Cumulative Sums (Cusum) Test) • тест на самую длинную серию «1» в блоке (Test for the Longest Run of Ones in a Block	• частотный блочный тест (Frequency Test within a Block) • тест на серию одинаковых бит (Runs Test) • тест на совпадение перекрывающихся шаблонов (Overlapping Template Matching Test) • тест на периодичность (Serial Test) • тест на линейную сложность (Linear Complexity Test) • спектральный тест (Discrete Fourier Transform Test) • универсальный статистический тест Маурера (Maurer Universal Test) • тест рангов бинарных матриц (Binary Matrix Rank Test) • тест приблизительной энтропии (Approximate Entropy Test) • тест на произвольные проходы (Random Excursions Test) • другой тест произвольные проходы (Random Excursions Variant Test) • тест на самую длинную серию «1» в блоке (Test for the Longest Run of Ones in a Block)
3.	DIEHARD	-	• проверка промежутков между днями рождений (The Birthday Spacing Test)
4.	TestU01	• тест веса Хэмминга (Hamming Weight Test) • тест автокорреляции (Autocorrelation) • тест случайных проходов (Random Walk Test) • тест на самую длинную серию «1» в блоке (Longest Run of 1's Test)	• тест веса Хэмминга (Hamming Weight Test) • тест серий и разрывов (Run and Gap Test) • тест сложности последовательности на основе алгоритма Лемпеля-Зива (Lempel-Ziv Complexity Test) • тест автокорреляции (Autocorrelations Test) • тест на самую длинную серию «1» в блоке (Longest Run of 1's Test) • CAT тест (CAT Test)
5.	Crypt-XS	• тест частот (Frequency Test) • тест бинарной производной (Binary Derivative Test)	• тест сложности последовательности (Complexity Test)

Предварительный анализ рассмотренных статистических тестов позволил определить, какие из них наиболее пригодны для использования в различных задачах разработки средств криптографической защиты информации.

Развитие методов статистического тестирования для некоторых классов ПСП. Анализ существующих пакетов для статистического тестирования приводит к выводу, что многие тесты могут успешно использоваться для исследования ПСП на случайность. Вместе с тем, особенности прикладных задач показывают, что классическая математическая модель статистического тестирования не вполне адекватно отражает потребности в исследовании некоторых объектов на случайность. Такая ситуация возникает, когда генерируемые последовательности могут обладать определенной структурностью. Например, последовательность разбивается на $m>1$ групп отрезков, где каждая группа получена в результате вычисления значений одной из m случайных

величин[1], относящихся к наблюдаемому случайному процессу. В таком случае исследуемую ПСП удобно представить в виде двумерного массива.

Опишем соответствующую математическую модель. Пусть имеется случайный или псевдослучайный процесс и связанные с ним случайные величины $\xi_1,\ldots,\xi_m$, имеющие в общем случае различные вероятностные распределения, $m>1$. В случайный момент времени t вычисляем значение случайной величины ξ_k и записываем в память двоичное представление вычисленного значения, $k=1,\ldots,m$. Пусть значение случайной величины ξ_k представляется d_k–разрядным двоичным числом, $k=1,\ldots,m$. Тогда в момент времени t генерируется двоичная последовательность длины $d=d_1+\ldots+d_m$. Если вычисления выполняются в моменты времени $t_1,\ldots,t_h$, $h>1$, то генерируется двоичная последовательность П длины dh или h двоичных последовательностей длины d. Воспользуемся вторым представлением.

Составим в памяти вычислителя таблицу размера $h\times d$. В ячейки k-го столбца таблицы записываются d_k–разрядные двоичные числа, соответствующие полученным значениям случайной величины ξ_k во все указанные моменты времени, $k=1,\ldots,m$. В ячейки r-й строки таблицы записываются двоичные числа, соответствующие полученным значениям случайных величин $\xi_1,\ldots,\xi_m$ в момент времени t_r, $r=1,\ldots,h$. Конкатенация двоичных слов, записанных в k-м столбце таблицы, образует двоичную последовательность длины d_kh, обозначим ее $Y_k^{\downarrow}$, $k=1,\ldots,m$. Конкатенация двоичных слов, записанных в r-й строке таблицы, образует двоичную последовательность длины d, обозначим ее $X_r^{\rightarrow}$, $r=1,\ldots,h$. Семейства $\{X_r^{\rightarrow}\}$ и $\{Y_k^{\downarrow}\}$ образуют двумерный массив. Таким образом, статистическое тестирование исходной последовательности можно выполнить как статистическое тестирование двумерного массива, позволяющее выявить более глубокие статистические закономерности по сравнению с тестированием исходной последовательности. Например, отклонение от ожидаемого вероятностного распределения в k-м столбце массива следует оценить случайную величину ξ_k как неподходящую для генерации элементов СП.

Возможно тестирование и для многомерных массивов. В указанном примере возникает тестирование 3-мерного массива, если для генерации двумерных массивов используются различные источники (возможно, аналогичной природы). Например, ПСП могут быть получены при взаимодействии идентичных программ с различными субъектами (пользователями).

Подход к тестированию многомерных массивов позволяет рассчитывать на более глубокое обоснование случайности генерируемых последовательностей. Преимуществом тестирования многомерных массивов является также принципиальная возможность высокой степени распараллеливания вычисления семейства статистик. Вместе с тем, возникают и новые сложности: требуется согласовать результаты тестирования различных фрагментов массива, согласовать результаты тестирования различных пользователей, выбрать наиболее подходящие для тестирования фрагменты и др. Эта область является перспективной для научных исследований.

СПИСОК ЛИТЕРАТУРЫ:

1. Архангельская А.В. Анализ подходов к определению термина «случайность» / А.В. Архангельская // Научная сессия МИФИ-2007. XIV Всероссийская научная конференция «Проблемы информационной безопасности в системе высшей школы»: сб. науч. тр. / Московский инженерно-физический институт (государственный университет). – М.: МИФИ, 2007. – С. 22 – 23.

[1] Здесь и далее под вычислением значения случайной величины ξ понимается испытание вероятностной схемы с аналогичным распределением, в результате которого получается одно из возможных значений величины ξ.

2. Агибалов, Г.П. Избранные теоремы начального курса криптографии / Г.П. Агибалов. – Томск: изд-во НТЛ, 2005. – 116 с.
3. Варфоломеев, А.А., Жуков А.Е., Пудовкина М.А. Поточные криптосистемы. Основные свойства и методы анализа стойкости / А.А. Варфоломеев, А.Е. Жуков, М.А. Пудовкина. – М.: ПАИМС, 2000. – 272 с.
4. Фомичев, В.М. Методы дискретной математики в криптологии / В.М. Фомичев. – М.: Диалог-МИФИ, 2010. – 424 с.
5. Блог Кода Безопасности: Статистические проверки случайных чисел методами NIST. [Электронный ресурс]. Режим доступа: http://habrahabr.ru/company/securitycode/blog/237695/ (дата обращения 25.02.2016)
6. Тесты псевдослучайных последовательностей и реализующее их программное средство [Электронный ресурс]. Режим доступа: http://www.tusur.ru/filearchive/reports-magazine/2012-25-2/108.pdf (дата обращения 25.02.2016)
7. Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Van- gel, M., Banks, D., Heckert, A., Dray, J., Vo, S. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Электронный ресурс]. Режим доступа: http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf (дата обращения 25.02.2016)

REFERENCES:

1. Arhangel'skaya A.V. Analiz podhodov k opredeleniyu termina «sluchaynost'» / A.V. Arhan-gel'skaya // Nauchnaya sessiya MIFI-2007. XIV Vserossiyskaya nauchnaya konferentsiya «Pro-blemy informatsionnoy bezopasnosti v sisteme vysshey shkoly»: sb. nauch. tr. / Moskovskiy inzhenerno-fizicheskiy institut (gosudarstvennyy universitet). – M.: MIFI, 2007. – S. 22 – 23.
2. Agibalov, G.P. Izbrannye teoremy nachal'nogo kursa kriptografii / G.P. Agibalov. – Tomsk: izd-vo NTL, 2005. – 116 s.
3. Varfolomeev, A.A., ZHukov A.E., Pudovkina M.A. Potochnye kriptosistemy. Osnovnye svoystva i metody analiza stoykosti / A.A. Varfolomeev, A.E. ZHukov, M.A. Pudovkina. – M.: PAIMS, 2000. – 272 s.
4. Fomichev, V.M. Metody diskretnoy matematiki v kriptologii / V.M. Fomichev. – M.: Dialog-MIFI, 2010. – 424 s.
5. Blog Koda Bezopasnosti: Statisticheskie proverki sluchaynyh chisel metodami NIST. [Eektronnyy resurs]. Rezhim dostupa: http://habrahabr.ru/company/securitycode/blog/237695/ (data obrashcheniya 01.03.2016)
6. Testy psevdosluchaynyh posledovatel'nostey i realizuyushchee ih programmnoe sredstvo [Elektronnyy resurs]. Rezhim dostupa: http://www.tusur.ru/filearchive/reports-magazine/2012-25-2/108.pdf (data obrashcheniya 01.03.2016)
7. Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Van- gel, M., Banks, D., Heckert, A., Dray, J., Vo, S. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Elektronnyy resurs]. Rezhim dostupa: http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf (data obrashcheniya 01.03.2016)