УДК 004.056.5:519.254

СИСТЕМА СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ ЭЛЕКТРОННЫХ ПЛАСТИКОВЫХ КАРТ

Н.Г. КИЕВЕЦ, А.И. КОРЗУН

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 3 мая 2012

Рассматриваются системы статистического тестирования генераторов случайных чисел. Предлагается система статистических тестов для генераторов случайных чисел электронных пластиковых карт.

Ключевые слова: электронная пластиковая карта, генератор случайных чисел, статистические тесты.

Введение

Современные информационные технологии передачи данных строятся с обязательным использованием личного идентификатора, в качестве которого наиболее целесообразно использовать электронные пластиковые карты (ЭПК) в различных форм-факторах.

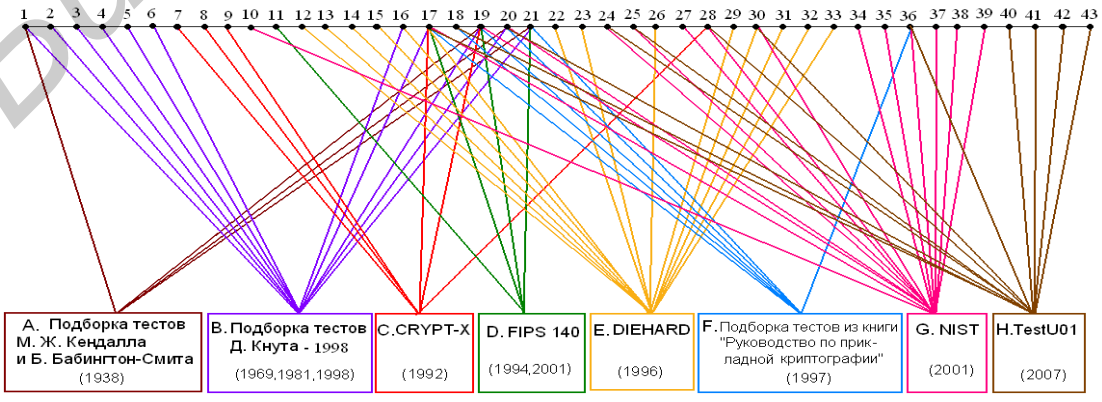
Особенностью ЭПК является наличие в их составе генераторов случайных чисел (ГСЧ), на основе которых вырабатываются ключи шифрования. Качество работы ГСЧ определяет качество ключей, а в целом криптостойкость передаваемых данных. Поэтому представляет интерес выбор и формирование системы тестов, с помощью которой целесообразно оценивать качество работы ГСЧ карт различных производителей.

Целью данной работы является рассмотрение существующих систем статистических тестов и формирование системы тестов для оценки качества работы ГСЧ.

Анализ подборок статистических тестов для оценки качества работы ГСЧ

В связи с большим объемом информации, описывающей каждый из тестов, в данной работе не приводится математического описания каждого из тестов. Тем не менее, ясно, что каждый тест представляет собой набор процедур.

На рисунке представлены наиболее известные подборки статистических тестов для исследования качества работы генераторов случайных чисел.



Подборки статистических тестов

Расшифровка тестов приведена ниже.

1. Тест интервалов (Gap test).
2. Тест конфликтов (Collision test).
3. Тест «максимум t» (Maximum-of-t test).
4. Тест сериальной корреляции (Serial correlation test).
5. Тест собирателя купонов (Coupon collector's test).
6. Тест перестановок (Permutation test).
7. Проверка бинарной производной (Binary derivative test).
8. Тест точек перехода (Change point test).
9. Тест сложности последовательности (Sequence complexity test).
10. Проверка кумулятивных сумм (Cumulative sums (Cusum) test).
11. Тест длинных подпоследовательностей (Long run test).
12. Тест на парковку (Parking lot test).
13. Обезьяньи тесты (Monkey tests).
14. Тест сжатия (Squeeze test).
15. Тест 3D-сфер (3D spheres test).
16. Тест промежутков между днями рождения (Birthday spacings test).
17. Тест подпоследовательностей (Run test или Runs test).
18. Проверка автокорреляции (Autocorrelation test).
19. Частотный тест (Frequency test).
20. Тест серий (Serial Test).
21. Тест покера (Poker test).
22. Тест пересекающихся сумм (Overlapping sums test).
23. Тест игры в кости (Craps test).
24. Спектральный тест (Spectral test).
25. Проверка сжатия при помощи алгоритма Лемпель-Зива (Lempel-Ziv complexity test или Lempel-Ziv compression test).
26. Подсчет числа единиц в определенных байтах (Count the 1's in specific bytes).
27. Проверка аппроксимированной энтропии (Approximate entropy test).
28. Проверка линейной сложности (Linear complexity test).
29. Проверка потока бит (Bitstream test).
30. Проверка рангов матриц (Binary matrix rank test).
31. Подсчет 1 в потоке байт (The count-the-1's test on a stream of byte).
32. Тест на минимальное расстояние (Minimum distance test).
33. Проверка пересекающихся перестановок (Overlapping 5-permutations test).
34. Частотный тест в подпоследовательностях (Frequency test within a block).
35. Проверка случайных отклонений (Random excursion test).
36. Универсальный тест Маурера (Maurer's «Universal Statistical» test).
37. Тест «блоков» в подпоследовательностях (Test for longest run of ones in a block).
38. Проверка пересекающихся шаблонов (Overlapping template matching test).
39. Проверка непересекающихся шаблонов (Non-overlapping template matching test).
40. Проверка случайных блужданий (Random walk test).
41. CAT-тест (CAT-test).
42. Проверка весов Хэмминга (Hamming weights).
43. Тест самой длинной последовательности (Longest run of 1's test).

Анализ наиболее часто употребляемых тестов, приведенных на рисунке, дает возможность увидеть, что тест подпоследовательностей 17 включен в 7 из 8 систем тестирования, частотный тест 19 входит в 6 из 8 приведенных систем, тест серий 20 содержится в 5 системах тестирования, тест покера 21 – в 4 системах. Все подборки содержат, по крайней мере, один из четырех перечисленных тестов. Данные тесты принято считать базовыми. Они использовались для исследования первых механических, физических и программных генераторов случайных чисел и используются в существующих системах тестирования, что подтверждается рисунком.

Первая подборка статистических тестов для оценки качества ГСЧ был опубликована в 1938 году М.Ж. Кендаллом и Б. Бабингтон-Смитом, которые предложили использовать четыре теста [1]: частотный тест, тест серий, тест покера и тест интервалов. Данные тесты являются

базовыми и включены в большинство существующих подборок тестов. Тесты были описаны для последовательностей десятичных чисел от 0 до 9, так как предназначались для оценки качества работы механических генераторов. На рисунке видно, что тест интревалов содержится еще лишь в подборке Д. Кнута. Однако, при использовании битовых последовательностей тест интервалов можно считать тестом подпоследовательностей. Действительно, интервал между единицами есть подпоследовательность нулей. В работе [2] подборка тестов М.Ж. Кендалла и Б. Бабингтон-Смита рассмотрена для случая битовых последовательностей.

Фундаментальной работой, на которую ссылаются большинство разработчиков статистических тестов, является второй том книги Д. Кнута «Искусство программирования» (The Art of Computer Programming) [3-5]. В нем представлена подборка тестов, которые традиционно применяются для исследования статистических свойств псевдослучайных последовательностей. Некоторые тесты рассмотрены для целочисленных последовательностей, а некоторые для последовательностей действительных чисел, принадлежащих интервалу (0;1). Тесты, описанные для последовательности чисел, принадлжащие интервалу (0;1), могут быть использованы также и для исследования битовых последовательностей. Например, в работе [6] тест интервалов подборки Д. Кнута описан для битовых последовательностей. Подборка Д. Кнута содержит все четыре теста набора М.Ж. Кендалла и Б. Бабингтон-Смита. В работе [6] отмечаются следующие недостатки подборки тестов Д. Кнута.

1. Отсутствие рекомендуемых параметров тестирования. Не совсем корректный выбор некоторых значений может привести к тому, что ряд тестов будет зависеть от длины исследуемой последовательности или браковать все последовательности.

2. Спорная методика оценки результатов. Д. Кнут предлагает считать последовательности, для которых вероятность появления данного результата лежит в интервалах [0;0,01] и [0,99;1], неслучайными, (0,01;0,1] и [0,9;0,99) – подозрительными на случайность, (0,1;0,9) – случайными. Таким образом, для истинно случайной последовательности вероятность должна стремиться к 0,5, хотя, как представляется, на самом деле она должна стремиться к 0.

Пакет статистических тестов Crypt-X [7] разработан исследовательским центром информационной безопасности Квинслендского университета технологий. Три из шести тестов являются распространенными и входят в подборки: тест 17 в подборки B, D, E, F, G и H, тест 19 входит в подборки A, B, F и G, тест 28 включен также в подборки G и H. Три теста не содержатся в других подборках.

Стандарт FIPS 140-1 [8] содержит четыре статистических теста, три из которых считаются базовыми (частотный тест, тест подпоследовательностей, тест покера) и тест длинных подпоследовательностей. Данную подборку можно использовать для контроля генераторов, но она малопригодна для статистической оценки генераторов. Более поздняя версия стандарта – FIPS 140-2 [9] содержит те же 4 теста, но с измененными диапазонами допустимых значений тестовых статистик. Недостатком подборки FIPS 140-1 является то, что для тестирования требуется непрерывная последовательность длиной 20000 бит. ГСЧ ЭПК не позволяет получить непрерывную последовательность такой длины.

Тесты DIEHARD были опубликованы в 1996 году на CD-ROM [10]. Система тестов DIEHARD предназначена для битовых последовательностей. Для некоторых тестов битовая последовательностей преобразуется в последовательность чисел, принадлежащих интервалу (0;1). В работе [6] авторы выделены следующие недостатки системы DIEHARD.

1. Описания некоторых тестов (а именно a parking lot test, the minimum distance test, 3Dspheres test, the squeeze test, the overlapping sums, the runs test и the craps test), не позволяют понять смысл этих тестов.

2. Параметры тестирования жестко заданы, например, размер области тестирования – независимо от размера файла анализируется определенное число байт.

3. Полностью отсутствует справочная служба и методика трактовки результатов.

4. Большинство тестов основано не на теоретических расчетах, а на результатах испытаний.

В работе [11] содержатся пять базовых тестов (частотный тест, тест серий, тест покера, тест подпоследовательностей и проверку автокорреляции), к которым добавлен универсальный тест Маурера. Отмечено, что тест Маурера может находить все отклонения от случайности, ко-

торые находят пять базовых тестов, но тест Маурера требует гораздо более длинных последовательностей.

Подборка тестов NIST [12] содержит 16 тестов. Система NIST содержит как базовые тесты, так и другие более мощные тесты, некоторые из которых включены в более ранние подборки (например, тест Маурера).

TestU01 [13] представляет собой библиотеку программ, предназначенных для статистического тестирования генераторов случайных равномерно распределенных чисел. Библиотека состоит из четырех модулей. Один из модулей содержит набор статистических тестов, в который включены классические тесты, другие тесты, приведенные в литературе, и несколько оригинальных тестов. Другой модуль библиотеки содержит шесть определенных подборок тестов. Три подборки предназначены для тестирования последовательностей действительных случайных чисел, равномерно распределенных на интервале (0;1). Три подборки предназначены для битовых последовательностей: Rabbit, Alphabit и Block Alphabit. Rabbit и Alphabit содержат 38 и 17 тестов соответственно. Подборка Block Alphabit предназначена для последовательностей, состоящих из блоков различной длины. Авторы подборок не утверждают, что подборки содержат независимые тесты, которые выявляют все возможные отклонения от случайности. Они считают, что трудно проверить независимость тестов и сравнить их эффективность. Тесты для подборок были выбраны в основном благодаря распространенности использования. В публикации [13] описаны некоторые тесты, содержащиеся в библиотеке TestU01 (отмечены на рисунке), но не приведены определенные перечни тестов, входящих в тестовые подборки.

Таким образом, рассмотрены восемь наиболее широко описанных в литературе подборок тестов. Существует система базовых тестов, входящих практически во все подборки. Система базовых тестов дополняется в каждой подборке своими специфическими тестами, отличающими одну подборку от другой.

Подборка тестов для оценки качества ГСЧ ЭПК

При выборе статистических тестов для оценки качества ГСЧ ЭПК необходимо учитывать следующие особенности:

- ГСЧ ЭПК являются физическими генераторами;
- ГСЧ ЭПК не вырабатывают непрерывную последовательность бит, а выдают случайные числа определенных длин.

Для эффективного тестирования необходимо использовать набор тестов, которые должны удовлетворять следующим условиям.

1. Тесты набора должны находить все возможные виды отклонений от случайности.
2. Тесты должны быть независимыми. Не следует использовать тестов больше, чем это необходимо.

Подборки М.Ж. Кендалла и Б. Бабингтон-Смита и FIPS 140 содержат тесты, которые широко распространены и считаются базовыми. Достоинством данных тестов является то, что для тестирования не требуется последовательностей большой длины. Использование тестов только данных подборок позволяют сделать предварительную оценку качества работы ГСЧ. Их целесообразно дополнить более сложными тестами, выявляющими широкий спектр аномалий в исследуемой последовательности.

Недостатки подборки Д. Кнута (отсутствие рекомендуемых параметров тестирования, спорная методика оценки результатов тестирования) требуют дополнительных доказательств применимости данной системы тестов для оценки качества работы ГСЧ ЭПК.

Пакет статистических тестов Crypt-X содержит три широкоупотребимых теста (частотный тест, тест подпоследовательностей, проверка линейной сложности), которые в том числе включены в систему NIST. Тест бинарной производной подборки Crypt-X в сущности является эквивалентом теста серий в случае пересекающихся серий. Тест сложности последовательности разработан для замены теста автокорреляции. Тест точек перехода предусматривает приближенное вычисление вероятности, погрешность которого не описана.

Подборка тестов из книги «Руководство по прикладной криптографии» практически входит в состав системы NIST.

Учитывая, что ГСЧ ЭПК не позволяет получить непрерывную битовую последовательность, следовало бы использовать подборку тестов для исследования последовательностей чи-

сел различной длины. Тесты DIEHARD предназначены исключительно для последовательностей чисел длиной 32 бита. Подборка тестов Block Alphabit из программной библиотеки TestU01 предназначена для исследования последовательностей, состоящих из блоков различной длины (2, 4, 8, 16 и 32 бита). Некоторые карты позволяют получить последовательность длиной 1-9, 16-25, 32 (ОСКАР), 48, 64, 80, 96, 112, 128,144 (MINOS) байта. Поскольку отсутствует четкое описание всех содержащихся в данных программах тестов, представляется сложным доказать правомерность их использования для тестирования карт ОСКАР и MINOS.

Система NIST практически лишена недостатков, присущих описанным выше системам. Кроме того, она обладает следующими достоинствами.

1. Данная подборка получила широкое распространение.
2. Все тесты предназначены для оценки битовых последовательностей.
3. Система включает в себя достаточно большое количество тестов – 16.
4. Тесты системы являются примерно независимыми [14].
5. Имеется подробное описание тестов с примерами и рекомендуемыми параметрами.
6. Система тестов создана относительно недавно – в 2001 году и вобрала в себя практически все достижения в области статистического тестирования ГСЧ.

В связи с вышеперечисленными достоинствами система NIST была взята за основу при создании системы тестирования ГСЧ ЭПК. Вследствие специфики ГСЧ ЭПК из системы NIST исключен тест 25, так как для тестирования необходимо знать параметры, которые не определяются теоретически. Эти значения получают, используя генератор с функцией SHA-1 в цепи обратной связи или генератор Blum-Blum-Shub.

Поскольку тест «Стопка книг» может эффективнее находить отклонения от случайности, чем тесты NIST [15], целесообразно сформировать систему тестов с учетом включения в нее теста «Стопка книг». Кроме того, при использовании данного теста последовательность разбивается на блоки, длина которых хорошо согласуется с длиной ключа, вырабатываемого ГСЧ ЭПК.

Таким образом, в окончательном виде система статистических тестов для оценки качества работы ГСЧ ЭПК состоит из тестов 10, 17, 19, 20, 24, 25, 27, 28, 30, 34, 35, 36, 37, двух вариантов теста 39 (см. рисунок) и теста «Стопка книг».

Заключение

Предложена система статистических тестов для генераторов случайных чисел электронных пластиковых карт. Система базируется на шестнадцати тестах, четыре из которых широко используются в других системах тестирования. Обосновывается использование тестов в предложенной системе тестирования.

STATISTICAL TESTING SYSTEM FOR PLASTIC CARDS RANDOM NUMBER GENERATORS

N.G. KIYEVETS, A.I. KORZUN

Abstract

The statistical testing system for plastic cards random number generators are considered. The system of statistical tests for plastic cards random number generators is offered.

Литература

1. *Kendall M.G.* // Journal of the Royal Statistical Society. 1938. Vol. 101, №1. P. 147-166.
2. *Isakson H.A.* // Generator of Random Numbers – Teleteknik. 1959.Vol. III, №2.
3. *Donald E. Knuth* // The Art of Computer Programming. 1969.
4. *Donald E. Knuth* // The Art of Computer Programming. 1981.
5. *Donald E. Knuth* // The Art of Computer Programming. 1998.
6. *Иванов М.А., Чугунков И.В.* Теория, применение и оценка качества генераторов псевдослучайных последовательностей. М., 2003.
7. *Caelli W., Dawson E., Nielsen L.* // CRYPT–X Statistical Package Manual, Measuring the Strength of Stream and Block ciphers. 1992.
8. Federal Information Processing Standards Publication 140-1. «Security Requirements for Cryptographic Modules» U.S. Department of Commerce/NIST. 1994.
9. Federal Information Processing Standards Publication 140-2. «Security Requirements for Cryptographic Modules» U.S. Department of Commerce/NIST. 2001.
10. *Marsaglia G.* // The Marsaglia Random Number CDROM including the DIEHARD Battery of Tests of Randomness. 1996.
11. *Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone* Handbook of Applied Cryptography. 1997.
12. *L'Ecuyer P., Simard R.* // Library for Empirical Testing of Random Number Generators. – ACM Transactions on Mathematical Software. 2007. Vol. 33. P. 32.
13. *Soto J.* // Proceedings of the 22nd National Information Systems Security Conference. 1999.
14. *Миненко А.И.* // Вестник СибГУТИ. 2010. №4. С. 36-46.