УДК 004.051

Р.Р. Вильданов, Р.В. Мещеряков, С.С. Бондарчук

Тесты псевдослучайных последовательностей и реализующее их программное средство

Статья посвящена методикам тестирования псевдослучайных последовательностей. Коротко описаны стандарты FIPS 140-2, NIST STS 800-22, набор статистических тестов Diehard, а также предложено программное средство для анализа и оценки качества псевдослучайных последовательностей.

Ключевые слова: тестирование псевдослучайных последовательностей, программное средство, FIPS 140-2, NIST STS, Diehard, ENT, D. Knuth, Practical Next Bit Test.

Псевдослучайная последовательность (ПСП) – последовательность чисел, которая была вычислена по некоторому определенному арифметическому правилу, но имеет все свойства случайной последовательности чисел в рамках решаемой задачи [1].

Генераторы ПСП являются важнейшими элементами любой системы защиты, надежность последней в значительной степени определяется именно свойствами используемых генераторов. Качественные ПСП, являясь по своей сути детерминированными, обладают тем не менее практически всеми свойствами реализаций истинно случайных процессов и успешно заменяют их, так как случайные последовательности чрезвычайно сложно формировать.

Тестирование генераторов случайных и псевдослучайных чисел (ГСЧ и ГПСЧ), используемых в криптографических приложениях, является актуальной задачей как в практическом, так и в теоретическом плане. Несмотря на значительные наработки в данной области, разработчики тем не менее нуждаются в удобном инструментарии, способном предоставить приемлемую метрику, которая позволит достаточно ясно исследовать степень случайности последовательностей, порождаемых ГСЧ (ГПСЧ), кроме того, обеспечить разработчиков достаточным объемом информации для принятия решения относительно «качества» генератора.

На сегодняшний момент разработано достаточно большое количество различных типов ГСЧ (ГПСЧ). Однако для демонстрации их статистических свойств использовались различные подходы к статистическому тестированию. Чаще всего набор и методику тестирования предлагал сам разработчик генератора. Таким образом, сложилась ситуация, которая характеризуется тем, что невозможно объективно сравнить различные генераторы с единых позиций. Выходом из этого положения является использование некоторого стандартного набора статистических тестов, объединенных единой методикой расчета необходимых показателей эффективности ГПСЧ и принятия решения о случайности формируемых последовательностей. Многообразие критериев оценки псевдослучайных последовательностей, используемых при шифровании, чрезвычайно велико. Каждый из подходов к анализу таких последовательностей можно отнести к одной из двух групп. Первая группа связана с поиском закономерностей, позволяющих воспроизвести шифрующую последовательность по относительно небольшому количеству материала. При этом основные требования сводятся к тому, чтобы в ПСП отсутствовали относительно простые межзнаковые зависимости. Вторая группа критериев связана с оценкой статистических свойств последовательности: имеется ли в исследуемой последовательности какой-либо частотный дисбаланс, позволяющий аналитику предположить значение следующего бита с вероятностью, большей 0,5. При этом свойства ПСП должны быть наиболее близки к свойствам истинно случайной последовательности, например в ПСП равномерно распределены не только отдельные знаки, но и m-граммы, т.е. набор m соседних знаков, m=1,2,… . Обе эти группы методов анализа последовательностей составляют системный подход к разработке поточных шифров и тестов, предназначенных для выявления различного рода дефектов в исследуемых ПСП [2].

Обзор существующих методик тестирования

В настоящее время для тестирования ПСП разработано несколько программных продуктов, которые содержат комплексы тестов для проверки различных статистических свойств. Рассмотрим некоторые из них.

В США был сделан первый шаг к стандартизации набора статистических тестов путем принятия в 1994 г. национального стандарта «Требования безопасности к криптографическим модулям» [2]. Однако требования и методика стандарта больше носят технологический характер. Они направлены на решение задачи статистического контроля используемых в криптографических модулях псевдослучайных последовательностей и в общем случае малопригодны к решению задачи исследования статистических свойств ГПСЧ.

Тесты Diehard – это набор статистических тестов для измерения качества набора случайных чисел. Они были разработаны Джорджем Марсалья в течение нескольких лет и впервые опубликованы в 1995 г. на CD-ROM, посвященном случайным числам. Вместе они рассматриваются как один из наиболее строгих существующих наборов тестов [3].

В 1999 г. специалистами NIST (Национальный институт стандартов и технологий (НИСТ) США), в рамках проекта AES (Advanced Encryption Standard) был разработан набор статистических тестов «NIST STS» (NIST Statistical Test Suite) и предложена методика проведения статистического тестирования ГСЧ (ГПСЧ), ориентированных на использование в задачах криптографической защиты информации, которая, на взгляд многих специалистов в данной области, на настоящий момент наилучшим образом отвечает потребностям всех заинтересованных сторон. Пакет NIST STS включает в себя 15 статистических тестов, которые разработаны для проверки гипотезы о случайности двоичных последовательностей произвольной длины, порождаемых ГСЧ или ГПСЧ. Все тесты направлены на выявление различных дефектов случайности. Основным принципом тестирования является проверка нулевой гипотезы H_0, заключающейся в том, что тестируемая последовательность является случайной. Альтернативной гипотезой H_a - является гипотеза о том, что тестируемая последовательность не случайна. По результатам применения каждого теста нулевая гипотеза либо принимается, либо отвергается. Решение о том, будет ли заданная последовательность нулей и единиц случайной или нет, принимается по совокупности результатов всех тестов [4].

Описание разработанного программного средства

В связи с массовым распространением многоядерных процессоров появилась возможность параллельной обработки данных. Для программирования многопоточных приложений на многопроцессорных системах с общей памятью существуют несколько инструментов, сравнительная характеристика которых приведена в табл. 1.

Таблица 1

Критерии и инструменты параллелизма

Инструмент / Критерий	WinAPI	POSIX	boost	STL	Qt	OpenMP	Intel® Threading Building Blocks
Кроссплатформенность	–	–	+	+	+	+	+
Встроенность	+	+	–	+	–	+	–
Усложнение программирования	+	+	+	+	+	–	–
Бесплатность	+	+	+	+	+	+	–

Наиболее эффективным инструментом параллелизма среди перечисленных является открытый стандарт для распараллеливания программ OpenMP (Open Multi-Processing) [5]. В сравнении с Intel® Threading Building Blocks OpenMP является наиболее предпочтительным выбором с точки зрения сложности программирования, т.к. в используемых алгоритмах преобладают операции обработки массивов [6].

При использовании инструмента параллелизма OpenMP, оптимизации кода программы и флагов компиляции общее время, затрачиваемое на тестирование последовательностей, уменьшилось в 5 раз по сравнению с оригинальным программным средством для тестирования последовательностей. В табл. 2 приведена оценка времени, затрачиваемого на тестирование последовательности длиной 16 Мб оригинального и разработанного программных средств.

В разработанном программном средстве консолидированы, оптимизированы и распараллелены тесты NIST STS, Diehard, тесты Д. Кнута [7], тесты ENT [8], практический тест на следующий бит [9] и графические тесты (выполненные с использованием HTML5). Исходный код программного средства написан на языке высокого уровня C++ и компилируется с использованием GCC на ОС семейства Windows, GNU Linux, и POSIX-системах без изменения.

Таблица 2

Сравнительная оценка времени, затрачиваемого на тестирование последовательности

Тест	Время обработки псевдослучайной последовательности, с		Уменьшение времени обработки последовательности, раз
	Программное средство	NIST STS	
Frequency	0,21	0,54	2,51
Block Frequency	0,07	0,65	9,32
Runs	0,13	2,47	18,98
Longest Runs Of Ones	0,11	1,44	12,78
Rank	1,04	18,87	18,06
Discrete Fourier Transform	113,16	146,53	1,29
Non Overlapping Template Matchings	39,13	430,49	11,00
Overlapping Template Matchings	0,25	14,60	58,83
Linear Complexity	83,66	651,27	7,78
Serial	16,09	85,60	5,32
Approximate Entropy	13,60	36,15	2,66
Cumulative Sums	0,50	1,87	3,72
Random Excursions Variant	2,07	10,39	5,03
Random Excursions	1,15	2,41	2,09
Universal	15,51	16,27	1,05
Общее время	286,69	1419,55	4,95

Исходный код разработанного программного средства может использоваться как библиотека и встраиваться в криптографические модули для самотестирования [10].

Работа выполнена в рамках проекта 7.701.2011 (проект 1/12) при поддержке Министерства образования и науки Российской Федерации.

Литература

1. Харин, Ю.С. Математические и компьютерные основы криптологии: учеб. пособие / Ю.С. Харин, В.И. Берник, Г.В. Матвеев. – Минск: Новое знание, 1999. – 319 с.

2. Security Requirements For Cryptographic Modules [Электронный ресурс]. - Режим доступа: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf, свободный (дата обращения: 13.05.2012).

3. Brown R. Dieharder: A Random Number Test Suite [Электронный ресурс]. – Режим доступа: http://www.phy.duke.edu/ ~rgb/General/dieharder.php, свободный (дата обращения: 13.05.2012).

4. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Электронный ресурс] / A. Rukhin, J. Soto, J. Nechvatal et al. – Режим доступа: http://csrc.nist.gov/ publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf, свободный (дата обращения: 13.05.2012).

5. The OpenMP® API Specification For Parallel Programming [Электронный ресурс]. – Режим доступа: http://openmp.org/, свободный (дата обращения: 13.05.2012).

6. Intel® Threading Building Blocks, OpenMP* или потоки ОС? [Электронный ресурс]. – Режим доступа: http://software.intel.com/ru-ru/articles/intel-threading-building-blocks-openmp-or-native-threads/, свободный (дата обращения: 13.05.2012).

7. Кнут Д. Искусство программирования для ЭВМ. В 4 т. – 2-е bзд. – М.: Вильямс, 2007. – Т. 3. Сортировка и поиск. – 2000. – 824 с.

8. Walker J. ENT A Pseudorandom Number Sequence Test Program [Электронный ресурс]. – Режим доступа: http://www.fourmilab.ch/random/, свободный (дата обращения: 13.05.2012).

9. Yao A.C. Theory and application of trapdoor functions: extended abstract // Proc. 23rd IEEE Annual Symposium on Foundations of Computer Science. Chicago, 3–5 Nov. 1982. – Chicago: IEEE, 1982. – P. 80–91.

10. Ходашинский И.А. Методы нечеткого извлечения знаний в задачах обнаружения вторжений / И.А. Ходашинский, И.В. Горбунов, Р.В. Мещеряков // Вопросы защиты информации. – 2002. – № 1. – С. 45–50.

Вильданов Руслан Равилевич
Студент каф. КИБЭВС ТУСУРа
Тел.: 8-952-885-88-64
Эл. почта: r.r.vildanov@yandex.ru

Мещеряков Роман Валерьевич
Канд. техн. наук, доцент каф. КИБЭВС ТУСУРа
Тел.: (382-2) 90-01-11
Эл. почта: mrv@security.tomsk.ru

Бондарчук Сергей Сергеевич
Д-р физ.-мат. наук, проф/ ТТГПУ
Тел.: (382-2) 41-34-26
Эл. почта: office@keva.tusur.ru

Vildanov R.R., Meshcheryakov R.V., Bondarchuk S.S.
Tests of pseudo-random sequences and implementing their software

The article is devoted to methods of testing pseudo-random sequences. Briefly describes the standards for FIPS 140-2, NIST STS 800-22, a set of statistical tests Diehard, as well as the proposed software for analyze and estimate the quality of pseudorandom sequences.
Keywords: testing of pseudorandom sequences, a software, FIPS 140-2, NIST STS, Diehard, ENT, D. Knuth, Practical Next Bit Test.