МЕТОДИКА СРАВНЕНИЯ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЛОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ПО РЕЗУЛЬТАТАМ ТЕСТОВ NIST

Заливако С. С., Иванюк А. А.
ООО "СК хайникс мемори солюшнс Восточная Европа"
Кафедра информатики, Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: sergey.zalivako@sk.com, ivaniuk@bsuir.by

В работе представлена методика сравнения генераторов случайных числовых последовательностей на основе результатов статистических тестов NIST, которые преобразованы в числовые вектора. Предлагается вычислять метрику косинусного расстояния между полученными векторами, что позволит количественно сравнивать качество разрабатываемого генератора с устройствами, соответствующими стандартам NIST.

Введение

Генераторы случайных числовых последовательностей (ГСЧП) применяются в различных сферах информационных технологий: криптография, статистическая выборка, иммитационное моделирование, компьютерные игры и др. В зависимости от области использования к физической реализации ГСЧП могут предъявляться различные требования. В частности, для использования в криптографических приложениях ГСЧП должен соответствовать стандартам NIST (National Institure of Standards and Technologies) [1]. В соответствии с тестами NIST, разрабатываемый генератор может либо соответствовать стандарту полностью, либо не соответствовать по определенным качественным критериям (например, существенное различие по количеству нулей и единиц в генерируемой последовательности, коррелированность элементов последовательности и др.).

С другой стороны, в процессе разработки, как правило, генератор изначально не соответствует стандарту NIST, поэтому по мере улучшения характеристик было бы желательно иметь количественную оценку несоответствия. В связи с данной необходимостью был предложен метод сравнения результатов тестирования ГСЧП, основанный на вычислении метрики расстояния между числовыми характеристиками результата статистических тестов NIST. Представленный метод позволяет определить количественные различия между реализациями ГСЧП, качество которых априори различно и определяется их структурой.

I. Стандарт NIST для ГСЧП

В соответствии со стандартами NIST, ГСЧП включает в себя два обязательных элемента: источник случайности (Entropy Source) и генератор псевдослучайных числовых последовательностей (ГПСЧП) (Deterministic Random Bit Generator, DRBG). В свою очередь, источник случайности может быть дополнен блоком выравнивания (Conditioning Component), который, как правило, улучшает характеристики равномерности вырабатываемой случайной последовательности. ГПСЧП может быть реализован как блочный шифр (например, AES), либо хеш-функция (HMAC, SHA-256).

Набор статистических тестов NIST состоит из 15 типов тестов: частотный побитовый тест (Frequency Test), частотный блочный тест (Block Frequency Test), тест на последовательность одинаковых бит (Runs Test), тест на самую длинную последовательность единиц в блоке (Longest Run Test), тест рангов бинарных матриц (Rank Test), спектральный тест (FFT Test), тест на совпадение неперекрывающихся шаблонов (Non-Overlapping Template Test), тест на совпадение перекрывающихся шаблонов (Overlapping Template Test), универсальный статистический тест Маурера (Universal Test), тест на линейную сложность (Linear Complexity Test), тест на периодичность (Serial Test), тест приблизительной энтропии (Approximate Entropy Test), тест кумулятивных сумм (Cumulative Sums Test), тест на произвольные отклонения (Random Excursions Test), другой тест на произвольные отклонения (Random Excursions Variant Test).

Каждый тест проводится на заданном количестве выборок m и характеризуется 14 параметрами: количество выборок, на которых p-значение попадает в диапазон [0,0; 0,1); [0,1; 0,2); [0,2; 0,3); [0,3; 0,4); [0,4; 0,5); [0,5; 0,6); [0,6; 0,7); [0,7; 0,8); [0,8; 0,9); [0,9; 1,0]; p-значение по результатам статистического теста равномерности p-значений, полученных на m выборках; бинарное значение результата теста равномерности (0 – не пройден, 1 – пройден); доля выборок k из m, прошедших тест; бинарное значение, обозначающее превышение порога по выборкам, прошедшим тест (0 – порог не превышен, т.е. тест был пройден на недостаточном числе выборок, 1 – порог превышен). Таким образом, каждый статистический тест может быть представлен набором из 14 параметров. Каждый тип статистиче-

ского теста может проводиться различное число раз (например, частотный побитовый тест – 1 раз, тест на периодичность – 2 раза, тест на совпадение неперекрывающихся шаблонов – 148 раз). В связи с этим общее число тестов, производимых на сгенерированной последовательности равно 188, следовательно, один запуск генератора характеризуется $14 \times 188 = 2632$ параметрами.

II. Экспериментальное исследование

Качество итоговой случайной последовательности определяется исходным качеством источника случайности, которое усиливается применением ГПСЧП. Соответственно, изменение количественных характеристик источника случайности (например, числа выходных значений, тактовой системной частоты и др.) влияет на результат статистических тестов NIST.

Для проведения экспериментального исследования был разработан ГСЧП, состоящий из 32 одинаковых независимо работающих источников случайности, реализованных на основе физически неклонируемых функций (ФНФ). Выходы источников были поданы на входы 32-выходного ГПСЧП, в результате чего генератор вырабатывал 32-разрядные случайные числа. Были рассмотрены 32 конфигурации источников случайности: один из источников активен, 31 – вырабатывает константный нуль; два активны, 30 – вырабатывают константу; ..., 32 источника активны, ни один не вырабатывает константу. Для каждой конфигурации были получены случайные последовательности, состоящие из 40 млн бит, которые, в свою очередь были разделены на $m = 100$ выборок для тестирования пакетом NIST. В результате статистического тестирования для каждого из генераторов был получен вектор данных, состоящий из 2632 компонент. Между всеми полученными векторами попарно были вычислены косинусные расстояний, показанные на Рисунке 1.

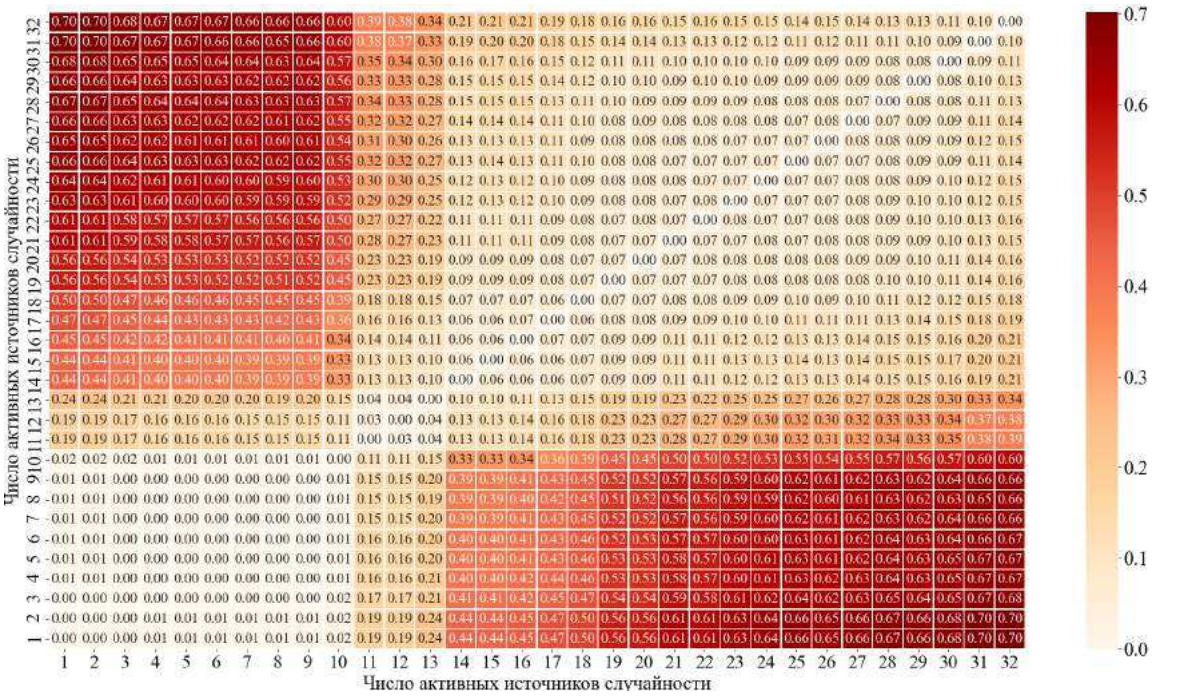

Рис. 1 – Таблица попарных расстояний между результатами тестов NIST

В результате эксперимента было показано, что генераторы с разным числом активных источников случайности существенно отличаются друг от друга. Сравнение результатов NIST-тестов с помощью метрики косинусного расстояния позволяет выделить три группы качества генераторов: низкое качество (генераторы с числом активных источников случайности от 1 до 10), среднее качество (11–13), высокое качество (14–32).

III. Заключение

Предлагаемый метод сравнения ГСЧП на основе вычисления метрики косинусного расстояния между числовыми векторами, характеризующими результаты тестирования NIST, позволяет разработчику количественно оценить разницу текущей версии генератора с устройствами, соответствующими стандартам NIST.

IV. Список литературы

1. A statistical test suite for random and pseudorandom number generators for cryptographic applications [Electronic resource]. – Mode of access: `http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf`. – NIST, 2010. – Date of access: 28.10.2021.