УДК 332.1

ОЦЕНКА КАЧЕСТВА ГЕНЕРАТОРА ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ НА ОСНОВЕ НЕЧЕТКОЙ ЛОГИКИ ДЛЯ ПРИМЕНЕНИЯ В ЭЛЕКТРОННОЙ КОММЕРЦИИ

Х.Х. Альнаджар,
Казанский национальный исследовательский
технический университет им. А.Н. Туполева-КАИ, г. Казань

Ключевые слова: *генератор псевдослучайных чисел, нечёткая логика, тесты на случайность, метод Монте-Карло, электронная коммерция.*

В настоящее время качественные генераторы псевдослучайных чисел ГПСЧ становятся важными для многих прикладных областей, включая телекоммуникационные технологии, информационную безопасность, электронная коммерция, моделирование и т.д. ГПСЧ с хорошими статистическими свойствами применяются для решения таких задач, как генерация криптографических ключей, реализация протоколов аутентификации, создание имитационных моделей и многих других.

Развитие деловой переписки и электронной коммерции требуют наличия методов обеспечения безопасности электронного документооборота. Электронные документы или финансовая информация передаются в компьютерных сетях и через Интернет в зашифрованном виде. Для обеспечения аутентичности, целостности и конфиденциальности обычно используются механизмы электронной цифровой подписи ЭЦП и шифрования данных. Самым важным аспектом шифрования является алгоритм генерации качественных псевдослучайных последовательностей.

Для формирования качественных последовательностей ГПСЧ должен генерировать так называемый «псевдослучайный шум». Для этого он должен удовлетворять критериям качества псевдослучайных последовательностей. В работах [1, 2] предложен новый генератор псевдослучайных чисел (НГПСЧ), использующий нечеткую логику и линейные регистры сдвига с обратной связью для получения псевдослучайных последовательностей.

Для оценки качества построенного НГПСЧ использовалось два известных пакета статистических тестов – DIEHARD, NIST [3] и численный метод Монте-Карло для сравнения построенного НГПСЧ и функции Randi пакета Matlab.

Общая структура предложенного НГПСЧ представлена на рис. 1.

Данный генератор состоит из двух LFSR, выходные данные которых поступают в два буфера размером 32 бит. Далее с помощью лингвистических переменных оцениваются статистические свойства информации, находящейся в буферах. Производится оценка:

- количества единиц в буфере (f_0);

- разности между числом блоков (f_1), состоящих из двух единиц (0110), и количества пробелов (f_2), состоящих из двух нулей (1001) в буфере $|f_1-f_2|$.

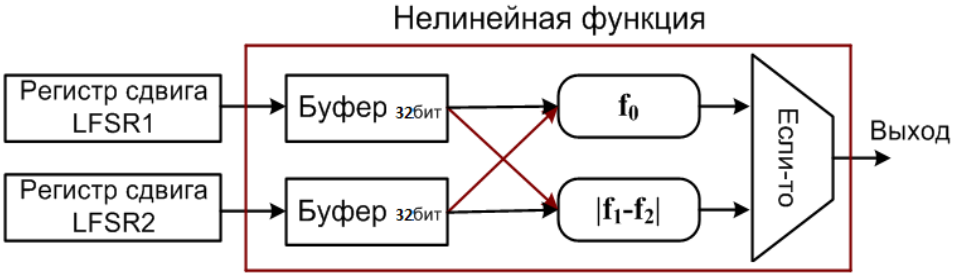

Рис. 1. Общая структура НГПСЧ

Далее работает совокупность ЕСЛИ-ТО правил для определения того, какой из регистров сдвига имеет лучшие статистические свойства на каждом шаге.

С целью повышения эффективности НГПСЧ были использованы следующие примитивные полиномы для реализации регистров сдвига с линейной обратной связью (LFSR) [4]:

$$P_1(x)=(1+x)(1+x^5)(1+x^{10})(1+x^{17})(1+x^{39})+x^{89}$$
$$P_2(x)=(1+x)(1+x^4)(1+x^7)(1+x^{20})(1+x^{53})+ x^{97}$$

Для того, чтобы предложенный НГПСЧ удовлетворяет всем критериям стойкости и безопасности против известных множеств атак [4], были внесены несколько изменений в функциях принадлежности лингвистических переменных f_0 и $|f_1-f_2|$.

Для оценки качества построенного НГПСЧ использовалось два известных пакета статистических тестов – NIST и DIEHARD. Далее построенный генератор сравнивался с рядом известных ГПСЧ включенных с пакетом DIEHARD. В заключении использовался численный метод Монте-Карло [5] для вычисления математической константы π с помощью двух генераторов – построенного НГПСЧ и функции Randi пакета Matlab, после чего выполнено сравнение точности формирования данной константы этими генераторами.

Для тестирования НГПСЧ были проведены численные эксперименты в соответствии с критериям прохождения тестов (среднее значение и дисперсия полученных p-values, Хи-квадрат, число неудачных подпоследовательностей). Сгенерированная с помощью НГПСЧ последовательность длиной 1024000 бит, разделена на 1000 подпоследовательностей длиной 1024 бита. К ним были применены выбранные ранее 5 наиболее важных статистических теста NIST. T1= "Частотный побитовый тест", T2= "Частотный блочный тест", T3="Тест на последовательность одинаковых битов", T4="Тест на самую длинную последовательность единиц в блоке", T5="Тест приблизительной энтропии". Все эксперименты реализованы в среде Matlab, версия R2012a (7.14.0.739) [8]. Результаты тестирования НГПСЧ представлены в табл. 1.

Таблица 1

Результаты тестирования подпоследовательностей, сгенерированных НГПСЧ

	Среднее значение, дисперсия (0.5,0.0833)		**Хи-квадрат** (≤ 21.667)	**Число неудачных последовательностей** (≤ 19)
T1	0.5029	0.0818	9.480	6
T2	0.5067	0.0812	11.040	5
T3	0.5028	0.0852	7.960	11
T4	0.4987	0.0818	14.200	5
T5	0.5001	0.0829	3.320	6

Из таблицы можно видеть, что псевдослучайные подпоследовательности, сгенерированные НГПСЧ, успешно прошли все тесты на случайность NIST.

С целью тестирования НГПСЧ с помощью пакета статистических тестов DIEHARD, последовательность с длиной 11 МегаБайт генерированы с помощью НГПСЧ и формированы надлежащим образом (двоичный файл целых чисел размером 32 бита) для тестирования с помощью пакетов тестов DIEHARD. Результаты тестирования сгенерированных последовательностей с помощью пакета тестов и DIEHARD, представлены в табл. 2.

Таблица 2

Результаты тестирования НГПСЧ с использованием пакета тесто DIEHARD

Название теста	**P-значение**	**Результат**
1. Дни рождения	0.4242	успех
2. Пересекающиеся перестановки	0.8351	успех
	0.6696	
3. Ранги матриц (31x31 и 32x32)	0.3742	успех
	0.3454	
4. Ранги матриц (6x8)	0.6937	успех
5. Обезьяньи тесты на 20 бит-слов	0.8979	успех
6. Обезьяньи тесты (OPSO, OQSO, DNA)	0.8054	успех
	0.9707	
	0.7693	
7. Подсчёт единиц в потоке байтов	0.8100	успех
	0.8255	
8. Количество единиц в конкретных байтах	0.5269	успех
9. Тест на парковку	0.2447	успех
10. Тест на минимальное расстояние	0.5139	успех
11. Тест случайных сфер	0.3793	успех
12. Тест сжатия	0.6126	успех
13. Тест пересекающихся сумм	0.1176	успех
14. Тест последовательностей (восходящие и нисходящие)	0.3551	успех
	0.1513	
15. Тест игры в кости (подсчитываются	0.3357	успех

победы, количество бросков в каждой игре)	0.9688	

Из данной таблицы видим, что НГПСЧ успешно прошел все тестов пакета DIEHARD.

Также было произведено сравнение предложенного НГПСЧ с 16 различными генераторами псевдослучайных чисел включенными в пакет DIEHARD. В результатах сравнение получено, что предложенный НГПСЧ показал наилучшие результаты по сравнении со всеми ГПСЧ пакета DIEHARD.

Были проведены также исследования с использованием метода монте-карло для оценки качества НГПСЧ. Использовался численный метод Монте-Карло для вычисления математической константы π с помощью двух генераторов – построенного НГПСЧ и функции Randi пакета Matlab, после выполнено сравнение точности формирования π этими генераторами. Математическую константу π можно вычислить путем генерирования случайных точек в квадрате и подсчета их части, которые лежат внутри вписанной четверти круга (рис.1). Вероятность попадания точки в круг = π/4.

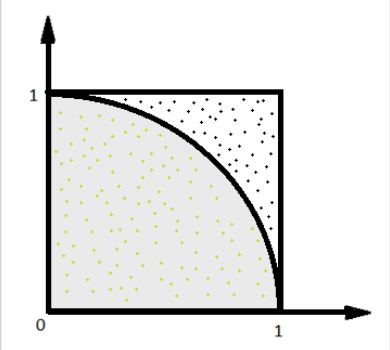

Рис. 1. Метод Монте-Карло приближенного вычисления константы π

В табл. 3 представлены результаты работы метода Монте-Карло для различных генераторов.

Таблица 3

Результаты применение метода Монте-Карло

Кол-во точек * Кол-во повторений	**средний (Randi)**	**STD (Randi)**	**средний (НГПСЧ)**	**STD (НГПСЧ)**
100*10000	3.1231	0.0185	3.1378	0.0040
1000*1000	3.1255	0.0161	3.1378	0.0065
10000*100	3.1249	0.0167	3.1378	0.0072
100000*10	3.1241	0.0175	3.1378	0.0069
1000000*1	3.1244	0.0172	3.1373	0.0043

Полученные результаты показали, что предложенный НГПСЧ работает лучше функции Randi, используемой в среде Matlab.

В данной статье показано, что предложенный генератор удовлетворяет статистическим критериям качества, а также формирует более качественные псевдослучайные последовательности, по сравнению 16 генераторами пакета

DIEHARD и функцией Randi пакета Matlab. Данный генератор может быть использован для решения практических задач во многих предметных областях (информационная безопасность, электронная коммерция, моделирование и т.д.).

Список литературы

1. *Аникин И.В., Альнаджар Х.Х.* Генератор псевдослучайных чисел, построенный на нечеткой логике // Информация и безопасность. 2015. № 3. Т. 18. С. 376–379.
2. *Anikin I.V., Alnajjar K.* Fuzzy stream cipher system // Proceedings of 2015 International Siberian Conference on Control and Communications, SIBCON 2015. Omsk, 2015.
3. *Вильданов Р.Р., Мещеряков Р.В., Бондарчук С.С.* Тесты псевдослучайных последовательностей и реализующее их программное средство // Доклады ТУСУРа. 2012. № 1 (25). Ч. 2. С. 108–111.
4. *Аникин И.В., Альнаджар Х.Х.* Анализ стойкости генератор псевдослучайных чисел, основанного на нечеткой логике, к корреляционным атакам // Информация и безопасность. 2016. № 3. Т. 19. С. 413–416.
5. *Соболь И.М.* Численные методы Монте-Карло. М.: 4-я типография, главная редакция физико-математической литературы изд-ва «Наука», 1973.