УДК 004.421.5

ТЕСТИРОВАНИЕ ПСЕВДОСЛУЧАЙНОГО ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ

ПИКУЗА М. О.

Белорусский государственный университет информатики и радиоэлектроники (г. Минск, Республика Беларусь)

E-mail: maksimpikuza@gmail.com

Аннотация. Рассмотрен опытный образец псевдослучайного генератора случайных чисел. Проведено его тестирование с использованием алгоритмов Национального института стандартов и технологий США. Показаны результаты тестирования в зависимости от периода снятия данных и величины обратного тока на шумовом диоде ND103L.

Abstract. A prototype pseudo-random generator of random numbers is considered. It was tested using algorithms from the US National Institute of Standards and Technology. Test results are shown versus sampling period, and reverse current across the ND103L noise diode.

Введение

Случайные последовательности чисел являются важной и неотъемлемой частью многих прикладных аспектов, таких как криптография, математическое моделирование, игровая индустрия [1]. Для получения случайных последовательностей применяют программные и аппаратные генераторы случайных чисел. Аппаратные генераторы случайных чисел основаны на внешнем источнике энтропии и зачастую состоят из источника энтропии, блока измерения и последующей обработки данных. В качестве источника энтропии можно использовать обратносмещенные шумовые диоды в диапазоне обратных токов выше пробивного, что позволяет получить наибольшую интенсивность электрических флуктуаций [2].

Основная часть

В изучаемом опытном образце псевдослучайного генератора случайных чисел (далее — ПГСЧ) основным элементом является шумовой диод ND103L, который имеет следующие технические характеристики:

- Постоянное напряжение шума (при токе 100 мкА) — 6-9 В;
- Спектральная плотность напряжения шума (при токе 50 мкА) — не менее 30 мкВ/√ Гц;
- Граничная частота (при токе 50 мкА) — не менее 1 МГц;
- Неравномерность спектральной плотности напряжения шума (при токе 50 мкА) — не более 3 дБ.

При подаче на шумовой диод обратного тока смещения выше пробивного, он начинает работать в режиме лавинного пробоя. В начальной стадии лавинного пробоя процесс ударной ионизации оказывается неустойчивым. Результатом случайной неравномерности генерации новых носителей заряда при ударной ионизации являются шумы, которые характерны для определенного диапазона токов. Эти шумы и являются источником энтропии для ПГСЧ.

Электрическая схема опытного образца ПГСЧ на шумовом диоде ND103L показана на рисунке 1. Рассматриваемый ПГСЧ работает следующим образом. На шумовой диод подается обратное напряжение выше напряжения пробоя (≥9 В). Величина обратного тока, протекающего через диод регулируется с помощью потенциометра и отображается на микроамперметре. Интенсивность электрических флуктуаций пропорциональна величине обратного тока. В результате лавинного пробоя на выходе конденсатора появляется случайный шумовой импульсный сигнал, который с помощью компаратора и делителя частоты преобразуется в двухуровневый случайный цифровой шум. Временные диаграммы напряжений в контрольных точках можно наблюдать и измерять основные электрические параметры с помощью цифрового осциллографа BORDO. Модуль ARDUINO на основе

микроконтроллера ATmega 2560 преобразует двухуровневый случайный цифровой шумовой сигнал в последовательность 0 и 1, которая передается на ПК и записывается в файл.

Для проверки генераторов случайных чисел используются как различные наборы тестов, анализирующие входную последовательность случайных чисел, такие как NIST (Национального института стандартов и технологий США) и Diehard [1,3], так и тесты, анализирующие сам источник энтропии [1].

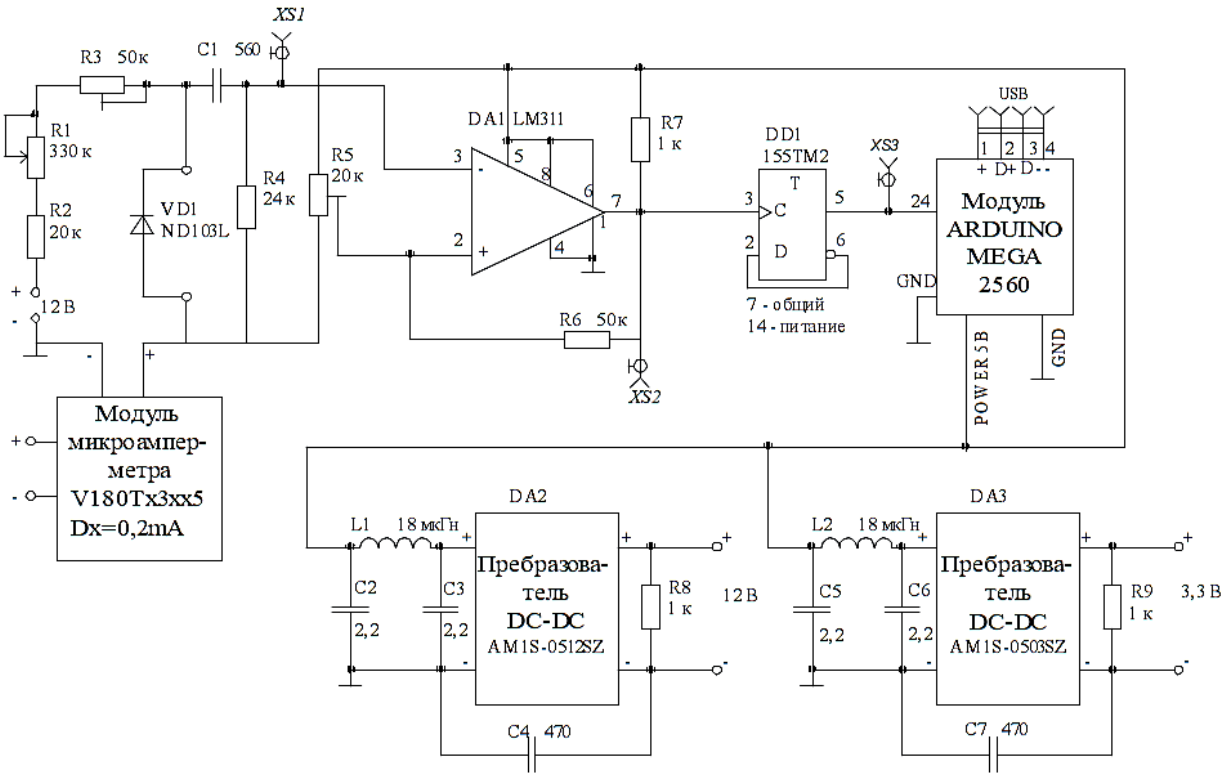

Рис. 1. Электрическая схема опытного образца ПГСЧ на шумовом диоде ND103L

В основе тестов NIST лежит понятие нулевой гипотезы, т.е. предположения, что между двумя фактами отсутствует какая-либо взаимосвязь. Существует также альтернативная гипотеза, которая опровергает нулевую гипотезу: т.е. между явлениями взаимосвязь существует. За нулевую гипотезу принимается предположение, что последовательность является истинно случайной, знаки которой появляются равновероятно и независимо друг от друга. Следовательно, если нулевая гипотеза верна, то генератор производит достаточно «хорошие» случайные числа.

При интерпретации результатов тестирования статистика последовательности, снятой с генератора, сравнивается с эталонной и если отклонение больше заданной погрешности p, то делается вывод, что нулевая гипотеза не верна с большей надежностью.

Набор тестов NIST содержит в себе 15 тестов: 1) частотный побитовый тест; 2) частотный блочный тест; 3) тест кумулятивных сумм; 4) тест на последовательность одинаковых битов; 5) тест рангов бинарных матриц; 6) тест на самую длинную последовательность единиц в блоке; 7) спектральный тест; 8) тест на совпадение неперекрывающихся шаблонов; 9) тест на совпадение перекрывающихся шаблонов; 10) универсальный статистический тест Маурера; 11) тест приблизительной энтропии; 12) тест на произвольные отклонения; 13) другой тест на произвольные отклонения; 14) тест на периодичность; 15) тест на линейную сложность [4].

Тестирование опытного образца ПГСЧ производилось с использованием тестов NIST при заданном значении погрешность p=0,01. Тестирование проводилось в несколько этапов при различных значениях входных параметров: T – период снятия значений, Iобр - обратный ток шумового диода. На каждом этапе снималась и тестировалась 100 последовательностей длиной 50000 бит, снятых с периодом T при токе Iобр.

Порядок снятия данных и тестирования был следующим: вначале снимались и тестировались данные при постоянном значении периода T и разных значениях тока Iобр, после чего снимались и

тестировались данные при постоянном значении тока Iобр и разных значениях периода T. Результаты тестированы представлены в табл. 1.

Таблица 1. Результаты тестирования опытного образца ПГСЧ

№	Параметры \ Результаты	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	**Σ**
1	T = 4 мкс, **Iобр = 20 мкА**	+	+	+		+	+	+	+	+						+	**9**
	T = 4 мкс, **Iобр = 40 мкА**		+		+	+	+	+	+	+						+	**8**
	T = 4 мкс, **Iобр = 60 мкА**		+		+	+	+		+	+		+			+	+	**9**
	T = 4 мкс, **Iобр = 80 мкА**		+			+	+	+	+	+	+				+	+	**9**
	T = 4 мкс, **Iобр = 100 мкА**						+	+								+	**3**
2	**T = 4 мкс**, Iобр = 50 мкА		+		+	+	+	+	+	+		+			+	+	**10**
	T = 20 мкс, Iобр = 50 мкА		+		+	+	+	+	+	+					+	+	**9**
	T = 40 мкс, Iобр = 50 мкА		+		+	+	+	+	+	+		+			+	+	**10**

При изменении исходных параметров генератора видно, что устройство относительно стабильно работает в диапазоне обратного тока через шумовой диод 20-80 мкА, а при увеличении тока далее количество проеденных тестов уменьшается, что говорит о увеличении неравномерности спектральной плотности напряжения шума с увеличением обратного тока через шумовой диод. Кроме того, видно, что при периоде снятия значений больше 4 мкс стабильность работы не уменьшается, что обусловлено тем, что частота выборки не превышает пределы граничной частоты равномерности спектра.

Заключение

Из общих результатов тестирования видно, что ПГСЧ проходит большую часть тестов NIST, что говорит о том, что данный генератор можно использовать в определенных сферах, однако его нельзя назвать истинно случайным и необходимо осуществить его доработку: усовершенствовать и более тщательно настроить аппаратную часть либо добавить программную реализацию алгоритмов постобработки данных, которая улучшит статистические характеристики потока данных.

Список использованных источников

1. Herrero-Collantes, M. Quantum Random Number Generators / M. Herrero-Collantes, J. C. Garcia-Escartin // Reviews of Modern Physics. – 2017. – №89(1).
2. Барановский, О. К. Кремниевые диоды-генераторы шумовых последовательностей : сб. научных трудов 2-й международной научной конференции «Материалы и структуры современной электроники» / О. К. Барановский [и др.]. 5-6 октября 2006. Минск. 2006. с. 58-61.
3. Hotoleanu, D. Real-Time Testing of True Random Number Generators Through Dynamic Reconfiguration / D. Hotoleanu, O. Cret, A. Suciu, T. Gyorfi, and L. Vacariu // 13th Euromicro Conference on Digital System Design: Architectures, Methods and Tools. – 2010. – P. 247–250.
4. A Statistical Test Suitefor Random and Pseudorandom Number Generators for Cryptographic Applications / National Institute of Standards and Technology. – Gaithersburg, Maryland, 2010.