ТЕСТИРОВАНИЕ КВАНТОВОГО ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ

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

Пикуза М.О.

Михневич С.Ю. – к.ф-м.н., доцент

Рассмотрен опытный образец оптического квантовый генератор случайных чисел. Проведено его тестирование с использованием алгоритмов Национального института стандартов и технологий США. Показаны результаты тестирования в зависимости от используемых тестов и размера выборки.

Формирование случайных последовательностей играет важную роль в современной технике, особенно в криптографии [1]. На практике используют программные и аппаратные генераторы случайных чисел. Любой аппаратный генератор использует внешний источник энтропии (шума). Источники шума, основанные на квантово-механических процессах являются абсолютно случайными, что делает генераторы, построенные на основе квантовых эффектов, наиболее достоверными [1,2].

Изучаемый опытный образец квантового генератора случайных чисел (далее – КГСЧ) состоит из светодиода (длина волны 635 нм), который при воздействии импульсов низкой интенсивности в результате квантовых процессов генерирует фотоны. Детектором фотонов является высокочувствительный кремниевый фотоэлектронный умножитель (далее – SIФЭУ), на выходе которого формируется аналоговый сигнал пропорциональный количеству зарегистрированных фотонов [3]. SIФЭУ отечественного производства преобразует излучение слабой интенсивности в последовательность импульсов при приложенном к нему обратном напряжении, превышающем напряжение пробоя (≥14 В). Обеспечена плавная регулировка обратного напряжения в пределах от 0 до 22 В. Для индикации напряжения использован цифровой вольтметр. Частота импульсов подсветки светоизлучающего диода (далее – СИД) 200 кГц, длительность импульсов — 1 мкс. Обеспечена плавная регулировка интенсивности подсветки SIФЭУ путем изменения прямого тока через светоизлучающий диод в пределах от 0,5 до 20 мА. Пороговый дискриминатор выделяет случайные импульсы с амплитудой ≥ 100мВ на выходе детектора фотонов. Делитель частоты преобразует выделенные импульсы в двухуровневый случайный цифровой шум. Временные диаграммы напряжений на выходах вышеперечисленных модулей 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 преобразуется в текстовый файл. Поскольку в основе генератора лежат квантовые события, то подобрав достаточно низкие значения прямого тока через светоизлучающий диод, можно добиться случайности последовательностей 0 и 1.

Генераторы случайных чисел, основанные на квантовых процессах, тестируются как с помощью тестов, анализирующих выходную последовательность случайных чисел (такие как тесты NIST (Национального института стандартов и технологий США) или Diehard тесты на случайность [1,4]), так и с использованием тестов, анализирующих сам источник энтропии [1]. При этом с учетом возможной деградации аппаратного генератора случайных чисел необходимо проводить тестирование до начала работы и в процессе.

Национальным институтом стандартов и технологий США изданы рекомендации по тестированию случайных и псевдослучайных генераторов [5]. В основе тестов 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. Если переходить к терминам случайных чисел, то 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.

С одной стороны, имеется статистика, подсчитанная на основе фактически собранных данных, т.е. по измеряемой последовательности. С другой стороны, есть эталонная статистика, получаемая математическими методами (теоретически вычисленная), которую бы имела истинно случайная последовательность. Очевидно, что собранная статистика не может сравняться с эталонной – насколько бы не был хорошим генератор, он все равно не идеален. Поэтому вводят некую погрешность, например, 5%. Она означает, что если собранная статистика отклоняется от эталонной больше чем на 5%, то делается вывод о том, что нулевая гипотеза не верна с большой надежностью.

Вместе с опытным образцом КГСЧ на основе 6-ти алгоритмов NIST, было реализовано программное обеспечение для тестирования случайных последовательностей с погрешностью в 1%. С помощью данной программы была протестирована последовательность чисел в размере 8192 бит. В определенном диапазоне значений обратного напряжения и тока светодиода все тесты (расчет автокорреляционной функции и тесты на основе алгоритмов NIST) дают положительный результат, что говорит о том, что исследуемая последовательность случайна (рисунок 1).

Вместе с тем, для использования опытного образца не в условиях лабораторных работ, а для криптографических применений необходимо использовать полный набор тестов NIST и, желательно, тесты, анализирующие сам источник энтропии.

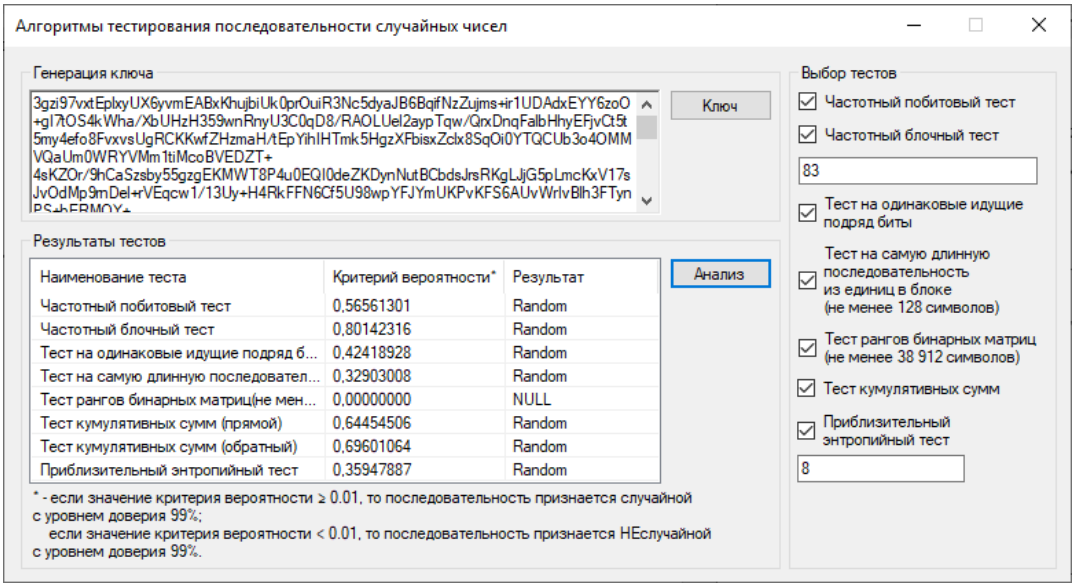

Рис. 1 – Результаты исследования последовательности из 8192 бит
с использованием 6-ти алгоритмов NIST

Для проведения полного тестирования необходимо, чтобы последовательность случайных чисел была не менее 10 Мб. Для того, чтобы снять такое количество значений в короткие сроки, была увеличена частота получения случайных бит из потока цифрового шума от КГСЧ. Полученная последовательность чисел была протестирована с помощью программного обеспечения, реализующего полный пакет тестов NIST. Результаты полного тестирования показали, что исследуемая последовательность чисел, снятая с опытного образца КГСЧ, не является случайной, что свидетельствует о необходимости более точного регулирования настроек квантового генератора и его дальнейшей модернизации.

В качестве возможной модернизации опытного образца КГСЧ можно реализовать автоматическую подстройку значений интенсивности подсветки СИД и обратного напряжения, приложенного к SIФЭУ. Это позволит перед непосредственным применением настроить КГСЧ на режим работы, в котором вероятность получить значения 0 и 1 будет стремиться к 0,5 с большей точностью.

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. Балыгин, К.А. Реализация квантового генератора случайных чисел, основанного на оптимальной группировке фотоотсчетов / К.А. Балыгин, В.И. Зайцев, А.Н. Климов, С.П. Кулик, С.Н. Молотков // Письма в Журнал экспериментальной и теоретической физики. − 2017. − Т. 106, вып. 7. − С. 451-458.

3. Барановский, О.К. Исследование возможности использования лавинных фотодиодов в режиме одноквантовой регистрации для создания квантовых генераторов случайных чисел / О.К. Барановский, О.Ю. Горбадей, А.О. Зеневич // Приборы и техника эксперимента. − 2018. − № 1. − С. 34-38.

4. 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.

5. A Statistical Test Suitefor Random and Pseudorandom Number Generators for Cryptographic Applications / National Institute of Standards and Technology. – Gaithersburg, Maryland, 2010.