ТЕСТИРОВАНИЕ ФИЗИЧЕСКИХ КВАНТОВЫХ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ

Тэт Наунг

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

Михневич С.Ю. – канд. физ.-мат. наук

В работе проведено тестирование физического генератора случайных чисел на основе светодиода. Доказано, что он не относится к IID типу, т.е. который выдает независимые и идентичные последовательности. В соответствии со стандартом для генераторов случайных чисел такого типа реализован тест на энтропию.

Случайные числа играют важную роль в кибербезопасности, защищенных коммуникациях, моделировании и статистическом моделировании. В отличие от генераторов псевдослучайных чисел (PRNG), которые полагаются на алгоритмы и начальные входные значения, квантовые генераторы случайных чисел (QRNG) используют присущую квантовым процессам неопределенность для получения недетерминированных и непредсказуемых выходных данных.[1]

По мере того, как эти устройства переходят к коммерческому использованию и интеграции в криптографические протоколы, становится необходимым проверить, что их выходные данные соответствуют стандартам случайности и энтропии, требуемым международными рекомендациями.

В работе проведена проведены тесты оценка данного генератора этой диссертации исследуется стандартизированная методология проверки физических QRNG, с упором на качество источника энтропии, используя NIST SP 800-90B в качестве эталонного стандарта.[2]

Для физических источников случайных чисел в соответствии со стандартом необходимо проводить не только тесты на случайность выходных последовательностей, но также оценивать и источник энтропии.

Источник энтропии QRNG состоит из трех компонентов:

источник шума: генерирует необработанное непредсказуемое поведение (например, квантовое);

компонент обработки (необязательно): увеличивает энтропию или устраняет смещение;

тесты работоспособности: мониторинг и обнаружение сбоев в генерации энтропии, при этом тестирование проводится до работы и в процессе работы. [1,2]

В изучаемом RNG второй компонент отсутствует, поэтому тесты на энтропию проводятся на выходной последовательности.

Оценка источника энтропии осуществляется на основе разных тестов в зависимости от того, относится ли данный тип RNG к IID, или нет. Для определения того, являются ли выходные последовательности IID, применяются статистические тесты. [2]

Обычно проверка на IID включает:

сбор не менее 1 000 000 образцов;

проведение тестов перезапуска (1000 перезагрузок по 1000 образцов каждая) для проверки согласованности и устойчивости в различных состояниях системы.

При проведении тестов отступили от нормы на количество образцов в связи, но даже для образцов (последовательностей) использованных для проведения статистических тестов получилось, что исследуемый RNG не является IID. [2]

Поскольку источник энтропии изучаемого QRNG выводит двоичные значения (0 или 1), оценка минимальной энтропии выполняется с использованием частотного анализа, в котором определяется min-энтропия:

$$Hmin = -log_2(max(P(0), P(1))). \quad (1)$$

применяется к 1 000 000-битному набору данных для оценки непредсказуемости каждого бита в худшем случае. Полученный результат 0,94 бита указывает на высококачественную случайность с низким смещением.

Список использованных источников:

1. Quantum Random Number Generators / M. Herrero–Collantes, J. C. Garcia–Escartin // Reviews of Modern Physics. – 2017. Vol.89, №1. – P. 1–54.

2. Национальный институт стандартов и технологий (NIST). «Рекомендации по источникам энтропии, используемым для генерации случайных битов (SP 800-90B)». — Гайтерсбург: NIST, 2018. — 78 с.

3. Пикуза М.О., Михневич С.Ю. «Тестирование квантового генератора случайных чисел» // Материалы 56-й научной конференции аспирантов, магистрантов и студентов БГУИР. — Минск: БГУИР, 2020. — С. 212.