А.Ю.СЕМЕНОВИЧ[1], ТЭТ НАУНГ[2]

ИССЛЕДОВАНИЕ ЭНТРОПИИ КВАНТОВОГО ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ

[1]*Учреждение образования «Белорусская государственная академия связи», г. Минск, Республика Беларусь, аспирант*

[2]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь, магистрант*

Залогом доверия к цифровым технологиям выступает защищенность персональных данных. Достигается она, в частности, за счет шифрования, надежность которого напрямую определяется криптографической стойкостью ключей. Формируются такие ключи генераторами случайных чисел (ГСЧ), а их стойкость означает невозможность предсказать очередные биты вырабатываемой последовательности. Все генераторы подразделяются на физические (истинные) и псевдослучайные алгоритмические. Псевдослучайные генераторы не обладают истинной энтропией, так как их характеристики полностью определяются начальным значением (seed), что делает их уязвимыми для криптоанализа. Поэтому растет интерес к физическим ГСЧ, основанным на источниках физического шума: тепловой шум, дробовой шум, фотонный шум. Однако все эти явления подвержены влиянию внешних факторов – температуры, напряжения питания, электромагнитных помех, что требует постоянной проверки работоспособности и качества генерируемой энтропии [1, 2].

Общеизвестные статистические тесты на случайность (NIST, FIPS, Diehard и др.) применяются для оценки качества случайности выходной последовательности бит. Однако для физических источников одной из проблем является уменьшение энтропии, вызванное деградацией параметров или изменением внешних условий. Уменьшение энтропии приводит к ошибкам, которые достаточно сложно обнаружить, поэтому рекомендуется применять тесты на оценку энтропии источника [3, 4]. Статистические тесты проверяют отсутствие закономерностей и равномерность распределения битов, тогда как оценка энтропии определяет

непредсказуемость источника. Физические ГСЧ могут иметь небольшой сдвиг (bias) или корреляцию между битами, которые тесты на случайность не замечают, но которые значительно снижают энтропию.

Исследование проводилось для источника энтропии физического генератора случайных чисел, построенного на основе светодиода [6, 7]. Генератор основан на квантовой природе света и использует фотодетекторы (лавинные фотодиоды или SiPM) для регистрации случайных фотонных событий. Слабый источник света генерирует случайные фотоны, детектор фиксирует их, преобразуя в электрический импульс; поскольку излучение фотонов — случайный процесс, электрические импульсы также случайно распределены во времени, формируя случайную последовательность. Последовательности, полученные с ГСЧ, проходят тесты NIST при точной настройке значений тока на фотодиоде и напряжения на Si-ФЭУ.

Все тесты, кроме проверки независимости для двоичных данных, были пройдены успешно. Согласно рекомендациям NIST, это не позволяет считать источник IID и применять к нему соответствующие методы оценки энтропии [5]. Таким образом, исследуемый источник является non-IID. Non-IID источники не являются неисправными — большинство реальных физических источников (термический шум, джонсоновский шум, кольцевые генераторы) по своей природе обладают свойствами non-IID из-за физических зависимостей и вариаций характеристик. Основная задача — правильно оценить уровень энтропии таких источников. Тестирование последовательностей с зависимыми значениями может привести к завышенным оценкам энтропии, однако большой и разнообразный набор оценок минимизирует вероятность значительного завышения.

Для оценки энтропии IID и non-IID используются тесты для определения min-entropy. Минимальная энтропия характеризует наименьшую теоретически возможную энтропию для данного источника и используется в криптографии как нижняя граница оценки безопасности. В случае источников non-IID в качестве итоговой оценки берется минимальное значение среди всех полученных оценок: оценка наиболее частого значения, оценка столкновений, марковская оценка, оценка сжатия, оценка t-кортежей, оценка самой длинной повторяющейся подстроки, оценка нескольких наиболее частых значений в диапазоне, оценка прогнозирования с запаздыванием, оценка MultiMMC, оценка LZ78Y. Оценка столкновений, марковская оценка и оценка сжатия применяются только к двоичным выходным данным.

Для исследуемого источника последовательностей двоичных чисел выполнялся тест столкновений (Collision Estimate). Он показывал значение энтропии, равное H1 = 6,4 бита. Согласно формуле (1), идеальное значение для 8-битовой системы составляет H = 8:

$$H = -\log_2 2^{-8}. \quad (1)$$

Для криптографии применяются ГСЧ с битовой энтропией 7,99–8,00 [9]. Учитывая, что для min-entropy берется наименьшее значение из трех тестов для битовой последовательности, а уже в тесте столкновений получена оценка ниже допустимой, можно сделать вывод, что данный ГСЧ не рекомендуется использовать для криптографических целей.

В отличие от энтропии Шеннона, min-энтропия определяет наихудшее значение энтропии, а не среднее, таким образом «раздвигая» границы вероятностей. Полученное значение min-entropy соответствует тому, что длина правильно предсказанной последовательности, соответствующей 99-му процентилю, составляет около 85 бит из 1000000 [1].

Таким образом, для ГСЧ на светодиоде было проведено исследование энтропии источника. Показано, что данный ГСЧ относится к non-IID источникам случайности. Для него рассчитано значение min-entropy. Несмотря на то, что исследуемый ГСЧ проходит статистические тесты на качество случайности, использовать его в криптографических целях не рекомендуется из-за малого значения min-entropy.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

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

2. Аппаратный генератор случайных чисел [Электронный ресурс] // Wikiwand. – URL: https://www.wikiwand.com/ru/articles/Аппаратный_генератор_случайных_чисел (дата обращения: 17.02.2026).

3. Rukhin, A. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, L. E. Bassham III. – Revision 1a. – Gaithersburg : National Institute of Standards and Technology, 2010. – 131 p. – (NIST Special Publication ; 800-22). – URL: https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final (date of access: 17.02.2026).

4. Barker, E. Recommendation for Random Number Generation Using Deterministic Random Bit Generators / E. Barker, J. Kelsey. – Revision 1. – Gaithersburg : National Institute of Standards and Technology, 2015. – 110 p.

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

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

7. Асаенок М.А., Зеневич А.О., Новиков Е.В. Исследование возможности использования кремниевых фотоэлектронных умножителей для создания генераторов случайных числовых последовательностей // Известия вузов. Электроника. 2020. Т. 25, № 2. – С. 114–122.