УДК 519.248:004.056.5

МЕТОД ОЦЕНКИ КАЧЕСТВА ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ ПО СПЕКТРАЛЬНОЙ ЭНТРОПИИ С БУТСТРЕП-ПОРОГАМИ И МЕТРИКОЙ МАХАЛАНОБИСА

Касьянов А.В.[1,2]
Научный руководитель – док. техн. наук, доцент Гришенцев А.Ю.[2]
[1]СПбГЭТУ «ЛЭТИ»
[2]Университет ИТМО
kasjanov@inbox.ru

Введение

Надёжность современных криптографических механизмов в значительной мере определяется эффективностью генераторов случайных и псевдослучайных чисел (Г(П)СЧ), поскольку именноМЕ они формируют случайные криптографические ключи, определяют параметры цифровых подписей и иные конфиденциальные данные, от которых зависит устойчивость алгоритмов шифрования и механизмов аутентификации.

Показателем качества случайных данных является энтропия битовой последовательности. Анализ энтропии выходных последовательностей, генерируемых Г(П)СЧ, позволяет формализовать предъявляемые к генераторам критерии непредсказуемости и вычислительной неотличимости от истинно случайных источников, что является обязательным условием для функционирования средств криптографической защиты информации (СКЗИ). При этом недостаточная энтропия или наличие статистических зависимостей может привести к уменьшению эффективного пространства ключей и значительному увеличению вероятности успешного проведения криптоанализа, что в критических случаях способно привести к полной компрометации системы. Исторический опыт свидетельствует, что недостаточное внимание к анализу энтропии или её некорректная оценка уже становились причиной значимых инцидентов в области информационной безопасности. Примером тому служит критическая уязвимость CVE-2023-39910 в библиотеке Libbitcoin Explorer версии 3.x [1], связанная со слабостью генерации энтропии при создании приватных ключей. Последняя уязвимость привела к инциденту Milk Sad в 2023 году, когда было восстановлено более 900,000 приватных ключей Bitcoin с прямыми финансовыми потерями свыше $0.8 миллиона.

Таким образом, расчёт и обоснование энтропии случайных битовых последовательностей является актуальной задачей, решение которой способствует повышению криптографической стойкости реализуемых протоколов и систем на основе случайных последовательностей. Целью настоящего исследования являлась разработка метода оценки энтропии случайных битовых последовательностей на основе анализа спектральной плотности мощности.

Основная часть

Методы исследования состояли из применения спектрального анализа битовых последовательностей на основе теоремы Винера–Хинчина [2] для вычисления спектральной плотности мощности и последующего расчёта спектральной энтропии [3]; использования непараметрического метода Бутстреп [4] для построения эмпирических распределений оценок и определения порогов принятия решения; применения расстояния (метрики) Махаланобиса [5] для количественного сравнения исследуемых реализаций с эталонной областью и формализации критерия принадлежности к классу случайных последовательностей.

В ходе исследования введён и обоснован метод оценки качества Г(П)СЧ на основе спектральной энтропии, а также построено формализованное решающее правило, реализуемое через бутстреп-оценивание распределения статистик и применение метрики Махаланобиса в пространстве агрегированных признаков. Показано, что предложенный метод обладает повышенной устойчивостью по отношению к выбору параметров битовой группировки (размера слова) и к конечной длине выборки по сравнению с энтропией Шеннона, вычисляемой по частотам битовых слов. На тестовом примере детерминированной последовательности натуральных чисел установлено, что энтропия Шеннона может давать ложноположительное заключение о случайности, тогда как спектральная энтропия устойчиво выявляет неслучайность за счёт наличия выраженной спектральной структуры. На примерах физического генератора в различных режимах продемонстрировано, что предлагаемый метод выявляет деградацию качества при неверно выбранной рабочей точке и фиксирует улучшение после её корректировки, при этом результаты NIST STS в обоих случаях могут оставаться формально положительными.

В рамках проведённых испытаний установлено, что ГПСЧ на основе поточного алгоритма шифрования ChaCha20 удовлетворяет критерию спектральной энтропии, что по результатам данного метода интерпретируется как соответствие требованиям к криптографически применимым источникам случайности. В соответствии с [6] данный ГПСЧ считается надежным и безопасным для применения в криптографических приложениях.

Выводы

Выявленная зависимость между структурными особенностями спектральной плотности мощности и качеством генерируемых последовательностей позволяет рекомендовать данный метод для внедрения в процедуру сертификации генераторов в условиях ограниченного объема измерений, где традиционные статистические процедуры могут оказаться недостаточно информативными.

Таким образом, представленный метод является ценным дополнением к существующим инструментам анализа случайных процессов и способствует повышению безопасности криптографических систем за счет более точного выявления потенциальных дефектов в работе генераторов.

Литература

1. CVE-2023-39910 Detail [Электронный ресурс]. – Режим доступа: https://nvd.nist.gov/vuln/detail/CVE-2023-39910 (Дата обращения 26.02.2026).
2. Якубов В.П. Статистическая радиофизика: учебное пособие. – Томск: Изд-во НТЛ, 2006. 132 с.
3. Pan Y. N., Chen J., Li X. L. Spectral Entropy: A Complementary Index for Rolling Element Bearing Performance Degradation Assessment // Journal of Mechanical Engineering Science. 2009. Vol. 223, no. 5, P. 1223–1231. https://doi.org/10.1243/09544062JMES1224.
4. Эфрон Б. Нетрадиционные методы многомерного статистического анализа: сборник статей. – М.: Финансы и статистика. 1988. 261 с.
5. Khachumov M.V. Distances, metrics and cluster analysis // Scientific and Technical Information Processing. 2012. Vol. 39. P. 310–316. https://doi.org/10.3103/S0147688212060020.
6. Bastos D. C., Brasil Kowada L. A., Machado R. C. S. On pseudorandom number generators // Acta IMEKO. 2020. Vol. 9, no. 4, P. 128–135. https://doi.org/10.21014/acta_imeko.v9i4.730.