3. *Абдольванд, Ф.* Повышение эффективности распределения ключевой информации в перспективных информационных технологиях: дисс. ... канд. /Ф. Абдольванд. – Минск, 2011. – 95 с.

ОБ ОЦЕНИВАНИИ ЭНТРОПИИ ВЫХОДНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ ФИЗИЧЕСКОГО ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ

А. М. КАПУСТА, М. С. АБРАМОВИЧ, М. Н. МИЦКЕВИЧ, И. К. ПИРШТУК

Физический генератор – устройство, которое генерирует последовательность случайных чисел на основе измеряемых параметров протекающего физического процесса. Работа таких устройств часто основана на использовании надежных источников энтропии, таких как тепловой шум, фотоэлектрический эффект, квантовые явления и т. д. Чаще всего физические генераторы применяются в системах компьютерного моделирования для имитации стохастических процессов и в криптографии для выработки криптографических ключей.

Источник энтропии – ключевая компонента генератора, полностью обеспечивающая неопределенность выходной битовой последовательности. Выходные данные источника шума оцифровываются и представляют собой битовые строки одинаковой длины. Битовая последовательность, генерируемая источником энтропии, называется первичной битовой последовательностью.

Лучшим источником энтропии будут квантовые процессы, но разработка генераторов на их основе относительно сложна и дорогостояща. Существуют также более доступные для использования в генераторах источники энтропии: время между нажатием клавиш на клавиатуре, движения мыши, шум со встроенного микрофона, время между принятыми по сети пакетами и т. д.

Основная проблема физических генераторов заключается в том, что первичная последовательность генератора в большинстве случаев не обладает свойствами независимости и равномерной распределенности. Это вызвано особенностями физических процессов, используемых в генераторах. Данная проблема решается с помощью специальных алгоритмов, которые позволяют «улучшить» свойства первичной последовательности: например, выровнять долю нулей и единиц в битовой последовательности, увеличить уровень энтропии и пр. На этапе функционального преобразования первичная последовательность генератора преобразуется в выходную последовательность. Необходимо отметить, что применение специального функционального преобразования не является обязательным, если первичная последовательность уже обладает всеми необходимыми свойствами.

Многие физические генераторы могут со временем терять свои свойства (как из-за конструктивных особенностей – например, износа или повреждения микросхем, так и из-за особенностей физических процессов – например, уменьшение радиоактивности вещества со временем). Исходя из этого, тесты контроля работоспособности являются неотъемлемой частью генератора и предназначены для проверки корректности функционирования устройства перед использованием и во время использования в режиме реального времени.

При проведении испытаний физических генераторов необходимо оценить случайность выходной битовой последовательности и определить, является ли она последовательностью независимых равномерно распределенных случайных величин, для которых выполняется условие $p\{0\} = p\{1\} = 0{,}5$.

В настоящее время наиболее полное описание методов и алгоритмов статистического тестирования приведено в пакете статистических тестов [1] Национального ин-

ститута стандартов и технологий США (NIST). Также описание многих статистических тестов приведено в [2; 3]. Эти тесты основаны на различных статистических свойствах, присущих только равномерно распределенным случайным последовательностям.

При анализе качества физических генераторов случайных чисел наряду с оцениванием случайности актуальной является задача оценивания энтропии выходной последовательности генератора.

Энтропия отражает неопределенность, связанную с предсказанием значения наблюдений: чем больше энтропия, тем больше неопределенность в предсказании значений. Существует множество возможных вариантов подсчета энтропии, но в качестве основной оценки рекомендуется выбирать заниженную меру – минимальную энтропию [4]. Это связано с тем, что на практике требуется, чтобы генератор гарантировал заданный уровень энтропии.

Пусть случайная величина X, принимающая значения из множества $\{x_1, \ldots, x_M\}$ с вероятностью $p(x_i)$, $i = 1, \ldots, M$, имеет минимальную энтропию H, тогда вероятность наблюдения любого значения x_i, $i = 1, \ldots, M$, будет не больше, чем 2^{-H}. В приведенных обозначениях минимальная энтропия определяется следующим образом:

$$H = -\log_2\left(\max_i p(x_i)\right). \quad (1)$$

Предположим, наблюдается выборка независимых одинаково распределенных случайных величин. Для оценки минимальной энтропии применяется следующий алгоритм:

1) По выборке оценивается вероятность наиболее частого значения $p_{\max} = \max_i p(x_i)$:

$$\hat{p}_{\max} = \frac{N_{\max}}{N},$$

где $N_{\max}$ определяет частоту наиболее встречаемого значения в выборке.

2) Вычисляется верхняя граница доверительного интервала:

$$\hat{p}^*_{\max} = p_{\max} + \Phi^{-1}(1-\alpha)\sqrt{\frac{p_{\max}(1-p_{\max})}{N}}, \quad (2)$$

где $\Phi^{-1}(\cdot)$ – обратная функция стандартного нормального распределения, α – уровень значимости.

3) Минимальная энтропия оценивается по формуле (1), используя оценку вероятности наиболее частого значения (2), при этом величина энтропии не может превышать длину наблюдения W в битах:

$$H = \min\{\log_2 M, -\log_2 \hat{p}^*_{\max}\}. \quad (3)$$

В случае, когда выборка не является последовательностью независимых одинаково распределенных величин, оценить минимальную энтропию довольно сложно. В [4] предлагается строить эмпирические оценки минимальной энтропии на основе статистических тестов.

Тест коллизий позволяет получить оценку минимальной энтропии на основе разности моментов времени, когда наблюдается совпадение (коллизия) двух наблюдений выборки. С использованием теста частичных коллекций строится оценка минимальной энтропии на основе того, сколько различных значений наблюдается в подвыборках, на которые разделяется исходная выборка. Тест сжатия позволяет получить оценку минимальной энтропии, основываясь на том, до какой степени можно сжать выборку. Частотный тест применяется для оценки минимальной энтропии на основе наиболее частого значения выборки. Оценку минимальной энтропии также можно получить, предполагая марковскую зависимость первого порядка между наблюдениями.

Оценку энтропии выходной последовательности физического генератора начинают с оценки энтропии первичной последовательности. Если предполагается, что

первичная последовательность является последовательностью независимых одинаково распределенных случайных величин, то необходимо подтвердить данный факт с помощью статистического тестирования. Если первичная последовательность проходит статистическое тестирование, то применяется алгоритм построения оценки минимальной энтропии для последовательности независимых одинаково распределенных случайных величин. В противном случае полагается, что она не является последовательностью независимых одинаково распределенных случайных величин и для построения оценки минимальной энтропии применяется второй алгоритм.

Тестирование независимости и одинаковой распределенности как первичной, так и выходной последовательности осуществляется с использованием статистических критериев хи-квадрат и перестановочных тестов [4]. Перестановочные тесты опираются на тот факт, что выборка, полученная перестановкой наблюдений исходной выборки, должна иметь те же свойства, что и исходная выборка.

Выходная последовательность обязательно должна быть последовательностью независимых одинаково распределенных случайных величин, поэтому она всегда проходит статистическую проверку на независимость и одинаковую распределенность. Если выходная последовательность не проходит статистическое тестирование, это означает, что генератор не прошел испытания.

При отсутствии дополнительного функционального преобразования первичной последовательности оценки минимальной энтропии выходной и первичной последовательностей совпадают. При реализации функционального преобразования на основе сертифицированных криптографических алгоритмов и функций проверяется корректность реализации. В случае корректности оценка минимальной энтропии рассчитывается по следующей формуле:

$$H = \min\{H_{in}, W_{out}\},$$

где H_{in} – энтропия, поступившая на вход преобразования, W_{out} – длина битовой строки на выходе.

В случае использования других алгоритмов и функций или некорректной реализации сертифицированных алгоритмов и функций применяется алгоритм построения оценки энтропии для последовательности независимых одинаково распределенных случайных величин.

Список использованных источников

1. National Institute of Standards and Technology special publication (SP) 800-22 A statistical test suite for random and pseudorandom number generators for cryptographic applications. – 2000.

2. Federal Information Processing Standard 140-2, Security requirement for cryptographic modules. – 2001.

3. *Knuth, D.* The art of computer programming / D. Knuth. – Vol. 2, 3rd ed. – Boston, USA, 1998.

4. National Institute of Standards and Technology special publication (SP) 800-90B Recommendation for the entropy sources used for random bit generation. – 2012.

НАУЧНО-МЕТОДИЧЕСКАЯ ПОДДЕРЖКА ДИСЦИПЛИНЫ «КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ» В РАМКАХ СПЕЦИАЛЬНОСТИ «КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ»

Е. Н. МЕЛЬНИКОВА

Криптографические протоколы представляют собой сравнительно молодое направление исследований в теоретической криптографии. Первые работы, посвященные