ИНТЕГРАЛЬНЫЙ КРИТЕРИЙ КАЧЕСТВА РАБОТЫ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

Келеберда В.С.
Научный руководитель – к.т.н., доц. Горелов Д.Ю.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки,14, каф. компьютерной радиоинженерии
и систем технической защиты информации (КРиСТЗИ),
тел. (057) 702-13-06, email: keleberda16@gmail.com.

It is proposed to use a complex criterion (uniformity, independence, stochasticity, cryptographic stability) for checking statistical properties of sequences of random numbers. As an integral criterion for the quality of generators of pseudorandom numbers, it is proposed to use the mathematical expectation of the number of tests passed by the sequences generated by the investigated RNG.

Базовым компонентом современных алгоритмов шифрования являются генераторы псевдослучайных последовательностей (ГПСП), которые во многом определяют их быстродействие и криптографическую устойчивость. Поэтому задача создания хороших генераторов и эффективных методов их оценки представляет большой интерес.

Для исследования ГПСЧ применяются две группы тестов: 1) графические; 2) оценочные. В первом случае статистические свойства последовательностей отображаются в виде графических зависимостей, по виду которых делают выводы о свойствах исследуемой последовательности случайных чисел. Во втором случае статистические свойства последовательностей определяются числовыми характеристиками. На основе оценочных критериев делаются заключения о степени близости свойств анализируемой и истинно случайной последовательностей. В отличие от графических тестов, где результаты интерпретируются пользователями, вследствие чего возможны различия в трактовке результатов, оценочные тесты характеризуются тем, что они выдают численную характеристику, которая позволяет однозначно сказать, пройден тест или нет.

На данный момент самым эффективным методом комплексного контроля является методика NIST STS. Она содержит 16 статистических тестов, совокупность которых предлагает критерии принятия решения относительно не только отдельной псевдослучайной последовательности (ПСП), но и относительно всего ГПСП. Основным недостатком NIST STS является сложность методики тестирования – рассчитываются 188 численных показателей, следовательно, ее нельзя рекомендовать для использования в реальном времени.

При разработке способов оценки качества ГПСП следует отметить следующие условия: 1) основной целью ГПСП является получение

последовательностей, которые ведут себя так, как будто являются случайными. Это означает что при проверке надо использовать критерии случайности: стохастичность, независимость, равномерность; 2) если n критериев подтверждают, что последовательность ведет себя случайным образом, это еще не означает, что проверка с помощью $(n+1)$-го критерия будет успешной. Однако каждая успешная проверка дает все больше и больше уверенности в случайности последовательности, следовательно, необходимо применять большое количество критериев.

В предложенном алгоритме оценка качества ГПСП осуществляется в два этапа. На первом этапе проверяется соответствие сгенерированных ГПСП последовательностей безусловным критериям стохастичности, независимости, равномерности и криптостойкости.

Проверка на равномерность производится с помощью χ^2-критерия (R_1), критерия Колмогорова-Смирнова (R_2) и частотного теста (R_3). Проверка на независимость проводится с помощью критерия монотонности (N_1), спектрального анализа на основе дискретного преобразования Фурье (N_2) и теста Маурера (N_3). Проверка на стохастичность производится с помощью эмпирических критериев интервалов (S_1), перестановок (S_2) и энтропийного теста (S_3). Проверка на криптографическую стойкость производится с помощью теста на следующий бит (KS_1). Если проверка пройдена, то соответствующий критерий равен единице, в противном случае – нулю.

Так как приведенные критерии являются безусловными, то интегральный критерий качества рассматриваемой ПСП может быть рассчитан по формуле:

$$K = R_1 \oplus R_2 \oplus R_3 \oplus N_1 \oplus N_2 \oplus N_3 \oplus S_1 \oplus S_2 \oplus S_3 \oplus KS_1, \quad (1)$$

где $\oplus$ – операция конъюнкции. Таким образом, считается, что исследовательская СВЧ прошла все проверки, если все критерии равны единице.

На втором определяется оценка самого ГПВЧ. Второй этап необходим, ведь большинство эмпирических статистических тестов предоставляет оценку только для конкретной последовательности, а не для источника, то есть генератора, этой последовательности. Считается, что исследуемый ГПВЧ прошел проверку, если математическое ожидание результатов тестирования статистических свойств сгенерированных им последовательностей является неизменным во времени и от реализации к реализации, т.е. генератор можно считать стационарным.

Список используемой литературы: 1. Вембо Мао. Современная криптография. Теория и практика. / Вембо Мао. Пер. с англ. – М.: Изд. дом «Вильямс», 2005. – 768 с. 2. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування: Монографія / І.Д. Горбенко, Ю.І. Горбенко. – Х.: Видавництво «Форт», 2012. – 880 с. 3. NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Електронний ресурс]. April 2000.