АНАЛИЗ СТАТИСТИЧЕСКИХ СВОЙСТВ ГЕНЕРАТОРА ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ НА ОСНОВЕ МНОГОМОДУЛЬНЫХ ПРЕОБРАЗОВАНИЙ

Гриненко Т.А., Макарчук Я.А., Стадченко Э.Ю.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Ленина, 14, каф. БИТ, тел. (057)7021425)
E-mail: bit@kture.kharkov.ua ; факс (057)7021425

The problem of construction of pseudo-random sequences with required properties is considered. Construction algorithm of such pseudo-random sequences is offered and theoretically justified.

Выходные данные генераторов случайных (ГСЧ) и псевдослучайных чисел (ГПСЧ) используются во многих криптографических приложениях, например, при генерации ключей, общесистемных параметров и др. В соответствии с требованиями криптографических приложений эти генераторы должны удовлетворять ряду сложных и противоречивых требований [1]. Основными из этих требований являются: основание алфавита, период повторения, восстанавливаемость, псевдослучайные свойства, а также структурные свойства. К настоящему времени разработан ряд алгоритмов и средств формирования ПСП. Основной их особенностью является то, что они строятся для двоичного основания, то есть m=2. Известен также класс линейных m-ичных последовательностей [2]. Однако этот класс последовательностей обладает неудовлетворительными структурными свойствами в смысле значительной зависимости появления символов в последовательности. Так для определения закона формирования таких ПСП необходимо и достаточно получить безошибочно $2l$ символов, где l – база линейного рекуррентного регистра [3]. Поэтому весьма важной и необходимой является задача разработки математических алгоритмов и средств с заведомо необходимыми свойствами и основанием алфавита. К наиболее перспективному на наш взгляд классу таких преобразований относится класс многомодульных преобразований.

Общее правило формирования последовательности многомодульного преобразования в поле GF(P) имеет вид

$$\begin{aligned} a_i &= (a_{i-1} * \theta_\upsilon) \bmod (P), \\ b_i &= a_i \left(\bmod (P_1, P_2, \ldots, P_{n-1}, P_n, m)\right). \end{aligned} \qquad (1)$$

где a_i и a_{i-1} – i-ый и $(i-1)$-й элементы формируемой последовательности; θ_υ – υ-ый первообразный элемент поля GF(P); $P_1, P_2, \ldots, P_n$ – промежуточные модули; m – основание алфавита.

В соотношении (1) должно выполняться условие

$$P >> P_1 >> P_2 >> \ldots >> P_n >> m \geq 2 . \qquad (2)$$

причем P_n – произвольное основание алфавита символов формируемой ПСП.

Применение правила (1) позволяет, с одной стороны, существенно повысить кодовую устойчивость, то есть устойчивость против определения закона формирования ПСП, а с другой, формировать последовательность элементов с требуемым основанием алфавита.

В работе [4] доказано, что можно построить m-ичные ПСП сколь угодно большого периода, при этом также теоретически обосновано, что на всей длине периода появление любого числа из интервала [0, q-1] практически равновероятно, если выполняется условие (2) .

Для тестирования генератора ПСЧ на основе многомодульного преобразования использовалась методика NIST STS [5], которая включает в себя 16 статистических тестов. Эти тесты используются для проверки гипотезы о случайности двоичных последовательностей произвольной длины, порождаемых ГСЧ или ГПСЧ. По совокупности результатов всех тестов принимается решение о том, будет ли заданная последовательность нулей и единиц «случайной» или нет.

С использованием методики NIST STS было осуществлено тестирование 2 ПСП (1 – генератор одномодульного преобразования ($P_1=2^{1024}$), 2 – генератор двумодульного преобразования ($P_1=2^{1024}$, $P_2=2^{512}$)), а также проведено сравнение свойств этих ПСП со свойствами ПСП генератора псевдослучайных чисел BBS [5] (тестовая выборка, рекомендованная NIST).

Для тестирования были выбраны следующие параметры:

1. Длина тестируемой последовательности $n=10^6$ бит.
2. Количество тестируемых последовательностей $m=100$. Таким образом, объем тестируемой выборки составил $N=10^6 \times 100=10^8$ бит.
3. Уровень значимости $\alpha=0{,}01$.
4. Количество тестов $q=189$. Таким образом, статистический портрет генератора содержит 18900 значений вероятности P.

В идеальном случае при $m=100$ и $\alpha=0{,}01$ может быть отвергнута только одна последовательность из ста, т.е. коэффициент прохождения каждого теста должен составлять 99%. Но это слишком жесткое правило. Поэтому и применяется правило на основе доверительного интервала для r_j. Нижняя граница в этом случае составит значение $r_{\min}=0{,}96015$. С этих позиций были проанализированы результаты тестирования ПСП.

В табл. 1 приводятся данные по прохождению ПСП тестов по Правилу 1 [5].

Таблица 1

Генератор	Количество тестов, в которых тестирование прошли более 99% последовательностей	Количество тестов, в которых тестирование прошли более 96% последовательностей
BBS	134 (70,8%)	189 (100%)
1	145 (76,7%)	183 (96,8%)
2	135 (71,4%)	184 (97,4%)

Генераторы 1 и 2 имеют статистику, подобную BBS.

В табл. 2 представлены сводные результаты по прохождению генераторами тестов по Правилу 2 [5].

Таблица 2

Генератор	Количество тестов, в которых значение вероятности $P \le 0{,}01$	Количество тестов, в которых значение вероятности $P \le 0{,}001$
BBS	0	0
1	6	5
2	4	3

В таблице значения вероятности P сравниваются с уровнями значимости $\alpha = 0{,}01$ и $\alpha = 0{,}001$, т.к. это достаточно малые значения.

Полученные значения не совпадают с отрицательными выводами по правилу один [5].

Литература: 1. *Завадская Л.А., Фаль А.М.* Криптографически сильные генераторы псевдослучайных последовательностей // Безопасность информации.-1997.-№1.-С.7-11. 2. *Горбенко И.Д.* Свойства характеристических дискретных сигналов // Радиотехника и электроника № 2, 1990. 3. *Горбенко И.Д.* Теория дискретных сигналов. Ч 1. Оптимальные дискретные сигналы с одно-двух- уровневой ПФАК. Учебное пособие. МО СССР, 1983. 4. Сущность и математические свойства одного класса многомодульных преобразований / *Т.А. Гриненко // Радиоэлектроника и информатика. 1999. № 00. С. 00–00.* 5. *А. Потий, С. Орлова, Т. Гриненко*. Статистическое тестирование генераторов случайных и псевдослучайных чисел с использованием набора статистических тестов NIST STS // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р. С. 206-214.