УМЕНЬШЕНИЕ ВЕЛИЧИНЫ ПОСТОЯННОГО СМЕЩЕНИЯ ПОСЛЕДОВАТЕЛЬНОСТИ С ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ ПРИ ПОМОЩИ АЛГОРИТМОВ ПОСТОБРАБОТКИ

Пикуза М.О.

ОАО «КБ Радар» - управляющая компания холдинга «Системы радиолокации»
г. Минск, Республика Беларусь

Михневич С.Ю. – канд. физ.-мат. наук

В работе изучено влияние алгоритмов постобработки (метод исключающего ИЛИ, метод фон Неймона, метод H-функции) на бинарную последовательность, полученную с аппаратного генератора случайных чисел. Рассчитаны значения постоянного смещения распределения вероятностей исходной и полученных в результате постобработки последовательностей. Практическая величина смещения после применения алгоритмов уменьшилась, но на меньшее значение чем было теоретически рассчитано, что свидетельствует о скоррелированности выходного потока с генератора.

При эксплуатации аппаратный генератор случайных чисел (ГСЧ) может иметь распределение, отличное от равномерного. Это может быть связано с наличием постоянного смещения у источника энтропии ГСЧ либо с изменением внешних факторов, которые воздействуют на источник энтропии. Для улучшения статистических характеристик аппаратных ГСЧ применяют различные алгоритмы постобработки. Они позволяют уменьшить постоянное смещение последовательности, однако их применение часто ведет к уменьшению скорости генерации случайных чисел. Рассмотрим некоторые из алгоритмов постобработки [1].

Метод исключающего ИЛИ (XOR). Из входного потока берется два бита, над ними проводится операция исключающее ИЛИ, результат операции записывается в выходной поток.

Метод фон Неймана (Von Neumann). Из входного потока берется два бита, если они равны 01, то в выходной поток записывается 0, если равны 10, то записывается 1, иначе не записывается ничего.

Метод H-функции (H function). Из входного потока берется два байта: A1 и A2. В выходной поток записывается результат выполнения H-функции: H(A1, A2) = A1$\oplus$ RL(A1, 1) $\oplus$ A2, где $\oplus$ - операция исключающего ИЛИ, RL(A1, 1) - операция циклического сдвига влево на 1 байта A1.

Одной из характеристик случайной последовательности является величина постоянного смещения распределения вероятностей, которая для двоичного числа вычисляется как половина разности вероятностей появления 0 и 1. Теоретические значения величины постоянного смещения после применения рассмотренных алгоритмов постобработки можно оценить при помощи выражений [2], представленных в таблице 1, где e – величина смещения исходной последовательности.

Таблица 1 – Выражения для оценки смещения выходной последовательности.

	XOR	Von Neumann	H function
Выходное смещение	$2e^2$	0	$\leq 4e^3$

Для сравнения теоретических значений постоянного смещения с практическими была получена последовательность случайных чисел с аппаратного ГСЧ, построенного на шумовом диоде. К данной последовательности были применены рассмотренные алгоритмы постобработки, в результате чего были получены новые последовательности случайных чисел. Далее были вычислены теоретические и практические значения постоянного смещения исходной последовательности и полученных в результате алгоритмов постобработок. Результаты вычислений приведены в таблице 2.

Таблица 2– Теоретически и практические значения смещений выходных последовательностей.

	Hardware RNG		XOR		Von Neumann		H function	
	теор	практ	теор	практ	теор	практ	теор	практ
Выходное смещение	-	$1{,}059*10^{-3}$	$2{,}243*10^{-6}$	$7{,}255*10^{-5}$	0	$2{,}263*10^{-4}$	$\leq 4{,}752*10^{-9}$	$4{,}212*10^{-5}$

Из результатов вычислений видно, что рассмотренные алгоритмы постобработки на практике уменьшают смещение последовательности на 1-2 порядка, однако эти значения оказались больше, чем теоретически рассчитанные. Это может говорить о том, что выходной поток с генератора скорреллирован. Устранить корреляцию можно используя специальные методы постобработки.

Список использованных источников:

1.Avaroglu E., Tuncer T. A novel S-box-based postprocessing method for true random number generation / E.Avaroglu, T. Tuncer // Turk J Elec Eng & Comp Sci, 2020. – №28. – P. 288-301.

2. Kwok S., Ee Y., Chew G., Zheng K., Khoo K., Tan C. A Comparison of Post-Processing Techniques for Biased Random Number Generators / S. Kwok, Y. Ee, G. Chew, K. Zheng, K. Khoo, C. Tan // Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication, 2011. – P. 175-190.