http://dx.doi.org/10.35596/1729-7648-2022-20-7-43-47

Оригинальная статья
Original paper

УДК 621.382.2/.3

УЛУЧШЕНИЕ СТАТИСТИЧЕСКИХ ХАРАКТЕРИСТИК АППАРАТНОГО ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ ПРОГРАММНЫМ СПОСОБОМ

М. О. ПИКУЗА

Белорусский государственный университет информатики и радиоэлектроники
(г. Минск, Республика Беларусь)

Поступила в редакцию 16.09.2022

Аннотация. В качестве источника случайных чисел часто применяют аппаратные генераторы случайных чисел, работа которых основана на хаотически изменяющихся параметрах различных физических процессов. Статистические характеристики таких генераторов не всегда позволяют использовать их в сфере защиты информации. Для совершенствования этих показателей используют различные программные средства обработки выходных данных генератора. Исследована возможность улучшения статистических характеристик аппаратного генератора случайных чисел программным способом. Данный генератор построен на основе шумового диода ND103L и на выходе имеет случайную цифровую последовательность двоичных чисел. С целью совершенствования статистических характеристик выходной поток случайных чисел обрабатывался при помощи программного метода, основанного на вычислении конечных разностей высокого порядка. Данный метод позволяет получить более симметричное распределение случайных чисел, а также увеличить скорость их генерации. После обработки данные с исследуемого генератора имели лучшие статистические характеристики, что подтверждено тестами NIST и Diehard, также скорость генерации увеличилась более чем в пять раз. Результаты выполненных исследований могут быть полезны разработчикам аппаратных генераторов случайных чисел, которым требуется улучшить характеристики генератора.

Ключевые слова: аппаратный генератор случайных чисел, шумовой диод, набор статистических тестов, NIST, Diehard, конечная разность высокого порядка.

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.

Для цитирования. Пикуза М. О. Улучшение статистических характеристик аппаратного генератора случайных чисел программным способом. Доклады БГУИР. 2022. 20 (7). С. 43–47.

STATISTICAL CHARACTERISTICS IMPROVEMENT OF A HARDWARE RANDOM NUMBER GENERATOR BY A SOFTWARE METHOD

MAKSIM O. PIKUZA

Belarusian State University of Informatics and Radioelectronics (Minsk, Republic of Belarus)

Submitted 16.09.2022

Abstract. As a source of random numbers, hardware random number generators are often used, the operation of which is based on randomly changing parameters of various physical processes. The statistical characteristics of such generators do not always allow their use in the field of information security. To improve the statistical characteristics, various software tools for processing the output data of the generator are used. The purpose of this work is to study the possibility to improve the statistical characteristics of a hardware random number generator by software. The investigated hardware random number generator is based on the ND103L noise diode and has a random digital sequence of binary numbers at the output. To improve the statistical characteristics, the output stream of random numbers was processed using a software method based on the calculation of high-order finite differences. This method would allow one to get a more symmetrical distribution of random numbers, as well as increase the speed of their generation. After processing, the data from the generator under study have better statistical characteristics, which is confirmed by the NIST and Diehard tests, and the generation rate has also increased by more than 5 times. The results of this work may be useful to developers of hardware random number generators who need to improve the performance of the generator.

Keywords: hardware random number generator, noise diode, statistical test suite, NIST, Diehard, high-order finite difference.

Conflict of interests. The author declares no conflict of interests.

For citation. Pikuza M. O. Statistical Characteristics Improvement of a Hardware Random Number Generator by a Software Method. Doklady BGUIR. 2022. 20 (7), 43–47.

Введение

Случайные последовательности имеют большое значение во многих прикладных аспектах – в криптографии, математическом моделировании, игровой индустрии и др. Для формирования случайных последовательностей часто применяют аппаратные генераторы случайных чисел (ГСЧ). Получение случайных чисел в таких устройствах осуществляется на основе хаотически изменяющихся физических процессов, таких как тепловой и квантовый шум. Хаотически изменяющиеся процессы теоретически непредсказуемы, однако на практике на них могут влиять окружающая среда и измеряющая аппаратура, что в итоге приводит к ухудшению статистических характеристик ГСЧ. Одним из проявлений ухудшения характеристик ГСЧ является неравномерность распределения случайных величин, что выражается в разном соотношении 0 и 1 в выходной последовательности ГСЧ, что может быть критично в области защиты информации [1].

В [2] представлено тестирование аппаратного ГСЧ на основе шумового диода ND103L при помощи набора статистических тестов NIST. Установлено, что его статистические характеристики зависят от исходных параметров, таких как период снятия значений, обратный ток шумового диода и температура окружающей среды. В [2] в качестве одного из способов улучшения статистических характеристик ГСЧ предлагалось использовать программные алгоритмы постобработки выходной последовательности ГСЧ. Также в [2] реализован и применен метод улучшения характеристик ГСЧ, основанный на вычислении конечных разностей высокого порядка [3]. В результате применения метода были улучшены статистические характеристики ГСЧ и увеличена скорость генерации случайных чисел.

Реализация метода улучшения характеристик аппаратного генератора случайных чисел

Метод улучшения статистических характеристик аппаратного ГСЧ основан на вычислении конечных разностей высокого порядка. Применение данного метода приводит к увеличению как симметрии распределения случайных чисел, так и величины стандартного отклонения, а также скорости генерации случайных чисел [3].

Алгоритм программной реализации метода следующий. ПЭВМ от генератора принимает поток случайных двоичных чисел, объединенных по 8 бит, т. е. по байтам. Каждый полученный байт преобразуется в число размером 64 бит. Далее производится вычисление конечной разности N-го порядка над последовательностью 64-битных чисел. Вычисленное значение конечной разности преобразуется в положительное число и представляется в двоичном виде. От этого двоичного числа берется L младших бит и отправляется в выходной поток.

Реализованный метод применяли к опытному образцу аппаратного ГСЧ, построенного на основе шумового диода ND103L. Структурная схема ГСЧ показана на рис. 1, где $F_{\text{цш}}$ – частота цифрового шума. Данный генератор подключается к ПЭВМ и отправляет в виртуальный COM-порт поток случайных двоичных чисел, собранных в один байт. Подробное описание характеристик и принципа работы ГСЧ изложено в [2].

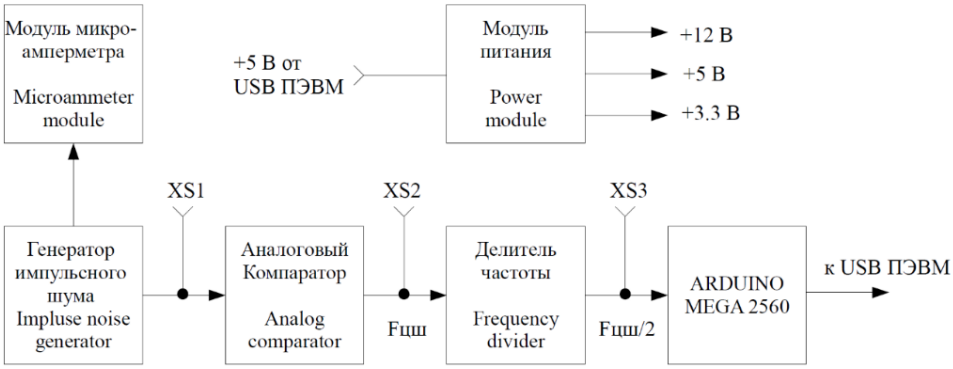

Рис. 1. Структурная схема опытного образца аппаратного генератора случайных чисел на шумовом диоде ND103L

Fig. 1. Structural circuit of a hardware random number generator prototype based on a noise diode ND103L

В ходе реализации метода было разработано специализированное программное обеспечение (ПО) для ПЭВМ, которое позволяло подключиться к виртуальному COM-порту и получить поток случайных чисел от ГСЧ в виде байт. Затем производили вычисления согласно описанному алгоритму и полученный поток случайных чисел отправляли в другой виртуальный COM-порт для дальнейшего использования в различных приложениях. Входной поток от ГСЧ и выходной поток после применения метода записывались в отдельные файлы для дальнейшего тестирования. Также в ПО можно задать порядок вычисляемой конечной разности N и количество младших бит L, отправляемых в выходной поток.

Тестирование метода улучшения характеристик аппаратного генератора случайных чисел

Для сравнения статистических характеристик последовательностей до и после применения метода использовали наборы статистических тестов от NIST и Diehard. Данные тесты позволяют исследовать различные типы отклонения от случайности, которые могут существовать в последовательности.

Набор тестов NIST содержал 15 статистических тестов:

1) частотный побитовый;
2) частотный блочный;
3) кумулятивных сумм;
4) на последовательность одинаковых битов;
5) на самую длинную последовательность единиц в блоке;
6) рангов бинарных матриц;
7) спектральный;

8) на совпадение неперекрывающихся шаблонов;
9) на совпадение перекрывающихся шаблонов;
10) универсальный статистический Маурера;
11) приблизительной энтропии;
12) на произвольные отклонения;
13) другой на произвольные отклонения;
14) на периодичность;
15) на линейную сложность [4].

Набор тестов Diehard содержал 18 статистических тестов:
1) дней рождения;
2) пересекающихся подстановок;
3) рангов бинарных матриц 31×31;
4) рангов бинарных матриц 32×32;
5) рангов бинарных матриц 6×8;
6) потока бит;
7) перекрывающихся пар с редким размещением;
8) перекрывающихся четверок с редким размещением;
9) ДНК;
10) подсчета единиц по байтам;
11) подсчета единиц в потоке;
12) на парковку;
13) на минимальное расстояние;
14) случайных сфер;
15) сжатия;
16) пересекающихся сумм;
17) последовательностей;
18) игры в кости [5].

Для проверки метода на опытном образце ГСЧ были установлены следующие исходные параметры: период снятия значений $T_с$ = 15 мкс; обратный ток шумового диода $I_{обр}$ = 20 мкА; температура окружающей среды $t_{окр}$ = 24 ºС. Данные параметры позволили получить наилучшие статистические характеристики ГСЧ [2]. В разработанном ПО задавались порядок конечной разности N = 47 и количество младших бит L = 45. Данные параметры позволяют получить максимальную скорость генерации случайных чисел, избегая появления корреляции в последовательности [3]. В ходе тестирования от ГСЧ было получено и записано в файл 55790000 бит случайных данных. После применения метода получено и записано в файл 312466632 бит случайных данных. Оба файла были протестированы с помощью наборов статистических тестов от NIST и Diehard. Результаты тестирования приведены в табл. 1, 2.

Таблица 1. Результаты тестирования аппаратного генератора случайных чисел тестами NIST
Table 1. Hardware random number generator NIST test results

Результат / Result	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	**Σ**
Исходная последовательность		+			+	+	+	+	+	+	+	+	+		+	**11**
Полученная последовательность	+	+	+	+	+	+	+	+	+	+	+	+	+		+	**14**

Таблица 2. Результаты тестирования аппаратного генератора случайных чисел тестами Diehard
Table 2. Hardware random number generator Diehard test results

Результат / Result	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	**Σ**
Исходная последовательность	+		?	+	+	+		+	+	+	+	+	+	+		+	+		**13**
Полученная последовательность	+	+	?	+	+	+	+	+	+	+	+	+	+	+		+	+		**15**

В табл. 1, 2 указаны результаты тестирования исходной и полученной последовательностей тестами NIST и Diehard. Успешно пройденные тесты отмечены символом «+» в соответствующих столбцах. В последнем столбце указана сумма всех успешно пройденных тестов для конкретной последовательности. Для тестов Diehard третий тест не проводился (отмечен символом «?»).

Заключение

Из результатов тестирования можно сделать следующие выводы:

– после выполнения алгоритма улучшились статистические характеристики потока случайных чисел, что подтверждается увеличением количества успешно пройденных тестов NIST и Diehard. Совершенствование характеристик связано с симметрированием распределения случайных значений и увеличением показателя стандартного отклонения после нахождения конечной разности высокого порядка;

– с помощью предлагаемого метода удалось увеличить скорость генерации случайных чисел в 5,6 раза, обеспечивая статистические характеристики не хуже исходных. Увеличение скорости происходит за счет того, что на каждые 8 бит данных от генератора случайных чисел с использованием рассматриваемого метода извлекается 45 бит.

Полученные результаты подтверждают, что предлагаемый метод можно применять в различных аппаратных генераторах случайных чисел с целью увеличения скорости генерации случайных чисел и улучшения статистических характеристик потока данных.

Список литературы / References

1. Herrero-Collantes, M. Quantum Random Number Generators / M. Herrero-Collantes, J. C. Garcia-Escartin // Reviews of Modern Physics. 2017. Vol. 89, No 1.
2. Пикуза, М. О. Тестирование аппаратного генератора случайных чисел при помощи набора статистических тестов NIST / М. О. Пикуза, С. Ю. Михневич // Доклады БГУИР. 2021. Т. 19, № 4. С. 37– 42. / Pikuza M. O., Mikhnevich S. Yu. (2021) Testing a Hardware Random Number Generator Using NIST Statistical Test Suite. *Doklady BGUIR.* 19 (4), 37–42 (in Russian).
3. Chizhevsky, V. N. Symmetrization of Single-Sided or Non-Symmetrical Distributions: the Way to Enchance a Generation Rate of Random Bits from a Physical Source of Randomness / V. N. Chizhevsky // Phys. Rev. E. 2010. Vol. 82, No 5.
4. A Statistical Test Suitefor Random and Pseudorandom Number Generators for Cryptographic Applications / A. Rukhin [et al.]. Gaithersburg: National Institute of Standards and Technology, 2010.
5. Brown, R. G. Dieharder: a Random Number Test Suite. Version 3.31.1 / R. G. Brown, D. Eddelbuettel, D. Bauer. http://webhome.phy.duke.edu/~rgb/General/dieharder.php.

Сведения об авторе

Пикуза М. О., аспирант кафедры информационных радиотехнологий Белорусского государственного университета информатики и радиоэлектроники.

Information about the author

Pikuza M. O., Postgraduate at the Department of Information Radiotechnologies of the Belarusian State University of Informatics and Radioelectronics.

Адрес для корреспонденции

220013, Республика Беларусь,
г. Минск, ул. П. Бровки, 6
Белорусский государственный университет информатики и радиоэлектроники
Тел. +375 33 650-31-78
E-mail: maksimpikuza@gmail.com
Пикуза Максим Олегович

Address for correspondence

220013, Republic of Belarus,
Minsk, P. Brovka St., 6
Belarusian State University
of Informatics and Radioelectronics
Tel. +375 33 650-31-78
E-mail: maksimpikuza@gmail.com
Pikuza Maksim Olegovich