http://dx.doi.org/10.35596/1729-7648-2021-19-4-37-42

Оригинальная статья
Original paper

УДК 621.382.2/.3

ТЕСТИРОВАНИЕ АППАРАТНОГО ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ ПРИ ПОМОЩИ НАБОРА СТАТИСТИЧЕСКИХ ТЕСТОВ NIST

М.О. ПИКУЗА, С.Ю. МИХНЕВИЧ

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

Поступила в редакцию 28 января 2021

Аннотация. Генераторы случайных чисел необходимы для работы систем криптографической защиты информации. В сфере защиты информации для корректного применения генератора необходимо, чтобы его выходная последовательность была неотличима от равномерно распределенной случайной последовательности. Для того чтобы в этом убедиться, необходимо провести тестирование выходной последовательности генератора с помощью различных наборов статистических тестов, таких как Dihard и NIST. Целью данной работы является тестирование опытного образца аппаратного генератора случайных чисел. Генератор построен на основе шумового диода ND103L и на выходе имеет случайную цифровую последовательность двоичных чисел. В опытном образце присутствует возможность регулирования величины обратного тока через шумовой диод, а также задания периода снятия данных, т. е. частоты генерации данных. В ходе работы с генератора был снят ряд последовательностей случайных чисел при различных значениях обратного тока через шумовой диод, периода снятия данных и температуры окружающей среды. Полученные последовательности были протестированы с помощью набора статистических тестов NIST. После анализа результатов тестирования был сделан вывод, что генератор относительно стабильно работает в некотором диапазоне исходных параметров, при этом ухудшение качества работы генератора за пределами этого диапазона связано с техническими характеристиками шумового диода. Также был сделан вывод, что исследуемый генератор применим в определенных приложениях, и для улучшения стабильности работы можно осуществить его доработку как в аппаратной части, так и программной. Результаты данной работы могут быть полезны разработчикам аппаратных генераторов случайных чисел, построенных по схожей схеме.

Ключевые слова: аппаратный генератор случайных чисел, шумовой диод, тестирование генератора случайных чисел, набор статистических тестов NIST.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Пикуза М.О., Михневич С.Ю. Тестирование аппаратного генератора случайных чисел при помощи набора статистических тестов NIST. Доклады БГУИР. 2021; 19(4): 37-42.

TESTING A HARDWARE RANDOM NUMBER GENERATOR USING NIST STATISTICAL TEST SUITE

MAKSIM O. PIKUZA, SVETLANA YU. MIKHNEVICH

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

Submitted 28 January 2021

Abstract. Random number generators are required for the operation of cryptographic information protection systems. For a correct application of the generator in the field of information security, it is necessary that its output sequence to be indistinguishable from a uniformly distributed random sequence. To verify this, it is necessary to test the generator output sequence using various statistical test suites such as Dihard and NIST. The purpose of this work is to test a prototype hardware random number generator. The generator is built on the basis of the ND103L noise diode and has a random digital sequence of binary numbers at the output. In the prototype there is a possibility of regulating the amount of reverse current through the noise diode, as well as setting the data acquisition period, i.e. data generation frequency. In the course of operation, a number of sequences of random numbers were removed from the generator at various values of the reverse current through the noise diode, the period of data acquisition and the ambient temperature. The resulting sequences were tested using the NIST statistical test suite. After analyzing the test results, it was concluded that the generator operates relatively stably in a certain range of initial parameters, while the deterioration in the quality of the generator's operation outside this range is associated with the technical characteristics of the noise diode. It was also concluded that the generator under study is applicable in certain applications and to improve the stability of its operation, it can be improved both in hardware and software. The results of this work can be useful to developers of hardware random number generators built according to a similar scheme.

Keywords: hardware random number generator, noise diode, random number generator testing, NIST statistical test suite.

Conflict of interests. The authors declare no conflict of interests.

For citation. Pikuza M.O., Mikhnevich S.Yu. Testing a hardware random number generator using NIST statistical test suite. Doklady BGUIR. 2021; 19(4): 37-42.

Введение

Потребность в случайных числах возникает во многих криптографических приложениях: в криптографических системах используются ключи, которые должны генерироваться случайным образом, а в криптографических протоколах случайные числа применяются для генерации цифровых подписей или создания задач при аутентификации [1].

В качестве источника случайных чисел используются аппаратные, программные или программно-аппаратные генераторы случайных чисел (ГСЧ). Генерация последовательности случайных чисел в аппаратных ГСЧ осуществляется на основе физических процессов, параметры которых меняются хаотически (например, тепловой или квантовый шум). Теоретически такие процессы абсолютно непредсказуемы, однако на практике на хаотические процессы могут влиять окружающая среда и измеряющая аппаратура, поэтому для обеспечения надежности полученные с помощью аппаратного ГСЧ случайные числа рекомендуется проверять специальными статистическими тестами [2].

При разработке аппаратного ГСЧ требуется правильно выбрать режим работы электрических компонентов генератора, позволяющий получать статистически случайные последовательности чисел. Для того чтобы выявить влияние на выходную последовательность ГСЧ различных параметров работы генератора, было проведено тестирование опытного образца аппаратного ГСЧ, построенного на основе шумового диода ND103L [3].

Методика тестирования аппаратного генератора случайных чисел

В качестве аппаратного ГСЧ для тестирования был взят опытный образец генератора случайных чисел, который построен на основе шумового диода ND103L. Структурная схема этого генератора представлена на рис. 1.

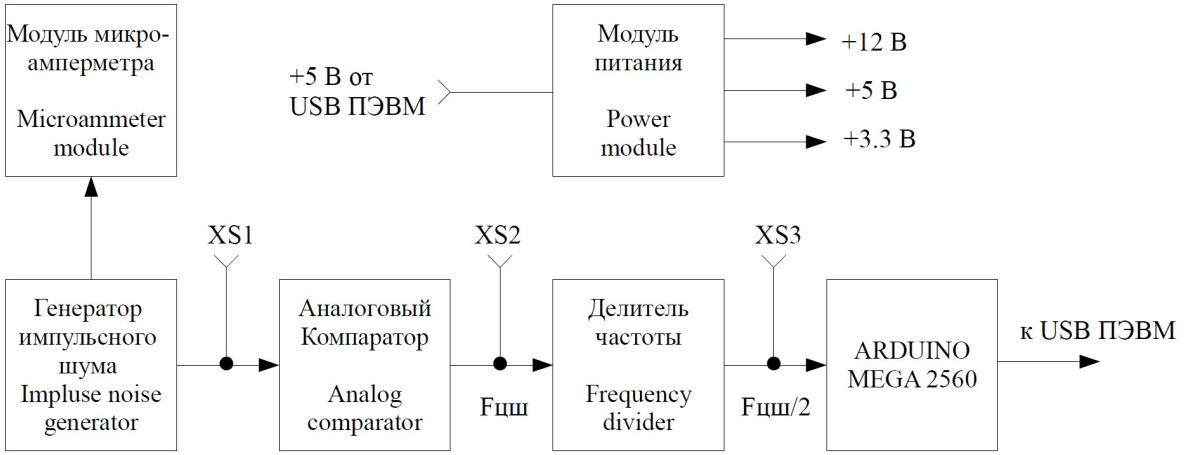

Рис. 1. Структурная схема опытного образца аппаратного ГСЧ на шумовом диоде ND103L
Fig. 1. Structural circuit of a hardware RNG prototype based on a noise diode ND103L

Основным элементом данного генератора является шумовой диод ND103L производства Республики Беларусь, который, согласно документации (URL.: https://integral.by/sites/default/files/diodi_generatori_shuma.pdf), имеет следующие технические характеристики:

– постоянное напряжение шума (при токе 100 мкА) – 6–9 В;
– граничная частота (при токе 50 мкА) – не менее 1 МГц;
– спектральная плотность напряжения шума (при токе 50 мкА) – не менее 30 мкВ/МГц;
– неравномерность спектральной плотности напряжения шума (при токе 50 мкА) – не более 3 дБ.

В начальной стадии лавинного пробоя, возникающего при превышении обратного тока смешения значения пробоя, процесс ударной ионизации носителей заряда оказывается неустойчивым. В результате неравномерности генерации новых носителей заряда возникающие шумы случайны для определенного диапазона токов. Эти шумы и являются источником энтропии для ГСЧ.

Тестируемый ГСЧ работает следующим образом. На шумовой диод подается обратное напряжение выше напряжения пробоя (≥9 В). Величина обратного тока, протекающего через диод, регулируется с помощью потенциометра и отображается на микроамперметре. Интенсивность электрических флуктуаций пропорциональна величине обратного тока. В результате лавинного пробоя на выходе конденсатора появляется случайный шумовой импульсный сигнал, который с помощью компаратора и делителя частоты преобразуется в двухуровневый случайный цифровой шум. С помощью цифрового осциллографа BORDO можно наблюдать и измерять основные электрические параметры в контрольных точках. Модуль ARDUINO на основе микроконтроллера ATmega 2560 преобразует двухуровневый случайный цифровой шумовой сигнал в последовательность 0 и 1, которая передается на ПЭВМ и записывается в файл.

Для проверки любых генераторов случайных чисел используются различные наборы тестов, такие как NIST (Национального института стандартов и технологий США) и Diehard. Для аппаратных ГСЧ используют также тесты, анализирующие сам источник энтропии [4].

Тестирование аппаратного генератора проводилось с использованием тестов NIST, позволяющих исследовать различные типы отклонения от случайности, которые могут существовать в последовательности. В основе тестов NIST лежит понятие нулевой гипотезы, т. е. предположения, что между двумя фактами отсутствует какая-либо взаимосвязь. В рамках

нулевой гипотезы элементы последовательности встречаются равновероятно и независимо друг от друга, т. е. последовательность является истинно случайной и ГСЧ производит «хорошие» случайные числа. При интерпретации результатов тестирования статистика последовательности, снятой с генератора, сравнивается с эталонной, и если отклонение больше заданной погрешности p, то делается вывод, что нулевая гипотеза не верна с большей надежностью. Чем больше выбирается значение погрешности p, тем менее достоверным является результат тестирования последовательности [1].

Порядок снятия данных с аппаратного генератора и их тестирования следующий. Вначале с генератора был снят ряд наборов двоичных данных при различных значениях исходных параметров: $T_с$ – период снятия значений, $I_{обр}$ – обратный ток шумового диода, $t_{окр}$ – температура окружающей среды. Смена исходных параметров происходила следующим образом: сначала снимались данные при постоянных значениях температуры $t_{окр}$ и периода $T_с$ и разных значениях тока $I_{обр}$, далее снимались данные при постоянных значениях температуры $t_{окр}$ и тока $I_{обр}$ и разных значениях периода $T_с$, после чего снимались данные при постоянных значениях периода $T_с$ и тока $I_{обр}$ и разных значениях температуры $t_{окр}$.

На каждом этапе было получено 55 последовательностей длиной 1 000 000 бит, снятых с периодом $T_с$ при токе $I_{обр}$ и температуре $t_{окр}$. Для тестирования алгоритмами NIST использовалось значение погрешности $p = 0{,}01$, которое применяется для криптографических целей [1]. Полученные последовательности двоичных данных при заданном значении погрешности были протестированы при помощи следующих тестов NIST: 1) частотный блочный тест; 2) тест на последовательность одинаковых битов; 3) тест на самую длинную последовательность единиц в блоке; 4) тест рангов бинарных матриц; 5) спектральный тест; 6) тест на совпадение неперекрывающихся шаблонов; 7) тест на совпадение перекрывающихся шаблонов; 8) универсальный статистический тест Маурера; 9) тест приблизительной энтропии; 10) тест на периодичность; 11) тест на линейную сложность [1].

Результаты тестирования аппаратного генератора случайных чисел

Результаты тестирования последовательностей, снятых с аппаратного ГСЧ при разных исходных параметрах, приведены в табл. 1.

Таблица 1. Результаты тестирования аппаратного ГСЧ
Table 1. Hardware RNG test results

№	Параметры / Результаты Parameters / Results	1	2	3	4	5	6	7	8	9	10	11	**Σ**
1	$t_{окр}$ = 24 ºС, $T_с$ = 15 мкс, ***I*_{обр} = 20 мкА**	+	+	+	+	+	+	+	+	+	+	+	**11**
	$t_{окр}$ = 24 ºС, $T_с$ = 15 мкс, ***I*_{обр} = 30 мкА**	+	+	+	+	+	+	+	+	+		+	**10**
	$t_{окр}$ = 24 ºС, $T_с$ = 15 мкс, ***I*_{обр} = 40 мкА**	+	+	+	+	+	+	+	+	+	+	+	**11**
	$t_{окр}$ = 24 ºС, $T_с$ = 15 мкс, ***I*_{обр} = 50 мкА**	+		+	+	+	+	+	+	+		+	**9**
	$t_{окр}$ = 24 ºС, $T_с$ = 15 мкс, ***I*_{обр} = 60 мкА**	+	+	+	+	+	+	+	+	+	+	+	**11**
	$t_{окр}$ = 24 ºС, $T_с$ = 15 мкс, ***I*_{обр} = 70 мкА**	+	+	+	+	+	+	+	+	+		+	**10**
	$t_{окр}$ = 24 ºС, $T_с$ = 15 мкс, ***I*_{обр} = 80 мкА**				+	+			+			+	**4**
2	$t_{окр}$ = 23 ºС, $I_{обр}$ = 20 мкА, ***T*_с = 15 мкс**	+	+	+	+	+	+	+	+	+	+	+	**11**
	$t_{окр}$ = 23 ºС, $I_{обр}$ = 20 мкА, ***T*_с = 30 мкс**	+	+	+	+	+	+	+	+	+	+	+	**11**
	$t_{окр}$ = 23 ºС, $I_{обр}$ = 20 мкА, ***T*_с = 45 мкс**	+	+	+	+	+	+	+	+	+	+	+	**11**
3	$T_с$ = 15 мкс, $I_{обр}$ = 20 мкА, ***t*_{окр} = 12 ºС**	+	+	+	+	+	+	+	+	+	+	+	**11**
	$T_с$ = 15 мкс, $I_{обр}$ = 20 мкА, ***t*_{окр} = 24 ºС**	+	+	+	+	+	+	+	+	+	+	+	**11**
	$T_с$ = 15 мкс, $I_{обр}$ = 20 мкА, ***t*_{окр} = 48 ºС**	+		+	+	+			+			+	**6**

В табл. 1 указаны результаты трех экспериментов, в ходе которых снимались и тестировались данные при изменении одного из параметров генератора. Успешно пройденные тесты отмечены символом «+» в соответствующих столбцах 1–11. В последнем столбце указана сумма всех успешно пройденных тестов при заданных исходных параметрах.

Обсуждение результатов тестирования аппаратного генератора случайных чисел

Из результатов тестирования можно сделать следующие выводы:

– генератор относительно стабильно работает в диапазоне обратного тока через шумовой диод 20–70 мкА, проходя большинство тестов, а при дальнейшем увеличении тока количество пройденных тестов уменьшается, что говорит о увеличении неравномерности спектральной плотности напряжения шума с увеличением обратного тока через шумовой диод;

– при изменении периода снятия значений количество пройденных тестов и соответственно стабильность работы генератора не изменяются. Это обусловлено тем, что частота выборки не превышает пределы граничной частоты равномерности спектра шумового диода;

– при увеличении температуры окружающей среды уменьшается число пройденных тестов и соответственно стабильность генератора, так как с увеличением температуры напряжение пробоя диода возрастает. Это происходит потому, что длина свободного пробега носителей заряда уменьшается, а следовательно, уменьшается энергия, которую носитель может приобрести на этом расстоянии в электрическом поле [5].

Полученные результаты говорят о том, что тестируемый аппаратный ГСЧ в широком диапазоне исходных параметров можно использовать в определенных приложениях. Для улучшения стабильности работы можно осуществить его доработку: усовершенствовать и более тщательно настроить аппаратную часть, а также добавить программную реализацию алгоритмов постобработки данных, которая улучшит статистические характеристики потока двоичных данных.

Список литературы

1. Rukhin A., Soto J., Nechvatal J., Smid M., Barker E., Leigh S., Levenson M., Vangel M., Hecket A., Dray J., Vo S. *A Statistical Test Suitefor Random and Pseudorandom Number Generators for Cryptographic Applications.* Gaithersburg: National Institute of Standards and Technology; 2010.
2. Будько М.Б., Будько М.Ю., Гирик А.В., Грозов В.А. *Методы генерации и тестирования случайных последовательностей.* СПб.: Университет ИТМО; 2019.
3. Буслюк В.В., Ворончук С.И., Лешкевич И.В. Режимы применения кремниевых генераторных диодов для создания широкоплосного шума. *5-я Международная научная конференция «Материалы и структуры современной электроники»*. 2012;1:24-27.
4. Herrero-Collantes M., Garcia-Escartin J.C. Quantum Random Number Generators. *Reviews of Modern Physics.* 2017;89(1).
5. Буслюк В.В., Нерода И.Ю., Петлицкий А.Н., Просолович В.С., Янковский Ю.Н., Лановский Р.А. Электрофизические параметры генераторных диодов для создания широкополосного шума. *Журнал Белорусского государственного университета. Физика*. 2017;1:95-99.

References

1. Rukhin A., Soto J., Nechvatal J., Smid M., Barker E., Leigh S., Levenson M., Vangel M., Hecket A., Dray J., Vo S. *A Statistical Test Suitefor Random and Pseudorandom Number Generators for Cryptographic Applications.* Gaithersburg: National Institute of Standards and Technology; 2010.
2. Budko M.B., Budko M.Yu., Girik A.V., Grozov V.A. [*Methods for generating and testing random sequences*]. St. Petersburg: ITMO University; 2019. (in Russ.)
3. Buslyuk V.V., Voronchuk S.I., Leshkevich I.V. [Modes of using silicon oscillator diodes to create wideband noise]. *Pyataya Mezhdunarodnaya nauchnaya konferenciya «Materialy i struktury sovremennoj elektroniki» = 5th International Scientific Conference* "*Materials and Structures of Modern Electronics*". 2012;1:24-27. (in Russ.)

4. Herrero-Collantes M., Garcia-Escartin J.C. Quantum Random Number Generators. *Reviews of Modern Physics.* 2017;89(1).
5. Busliuk V.V., Neroda I.Y., Pyatlitski A.N., Prasalovich U.S., Yankouski Y.N., Lanouski R.A. [Electrophysical parameters of the diodes for broadband noise generation]. *ZHurnal Belorusskogo gosudarstvennogo universiteta. Fizika = Journal of the Belarusian State University. Physics*. 2017;1:95-99. (in Russ.)

Вклад авторов

Пикуза М.О. получил ряд наборов данных с генератора при разных исходных параметрах, протестировал их с помощью тестов от NIST и сделал выводы.

Михневич С.Ю. выполнила постановку задачи, научное руководство.

Authors' contribution

Pikuza M.O. got a number of datasets from the generator with different initial parameters, tested them using tests from NIST and made conclusions.

Mikhnevich S.Yu. set out the problems and acted as a scientific advisor.

Сведения об авторах

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

Михневич С.Ю., к.ф-м.н, доцент кафедры информационных радиотехнологий Белорусского государственного университета информатики и радиоэлектроники.

Information about the authors

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

Mikhnevich S.Yu., PhD, Assosiate Professor 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 str., 6,
Belarusian State University
of Informatics and Radioelectronics;
tel. +375-33-650-31-78;
e-mail: maksimpikuza@gmail.com
Pikuza Maksim Olegovich