ТЕСТИРОВАНИЕ АППАРАТНОГО МОДУЛЯ ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ В СОСТАВЕ МИКРОКОНТРОЛЛЕРА СЕМЕЙСТВА STM32

Пикуза М.О.[1], аспирант

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Михневич С.Ю. – доцент, к.ф-м.н.

Аннотация. Собран макет для проверки аппаратного модуля генератора случайных чисел в составе микроконтроллера семейства STM32 на основе отладочной платы STM32F4DISCOVERY. Проведено тестирование модуля генератора случайных чисел с использованием набора тестов NIST. Показаны результаты тестирования в зависимости от размера выборки.

Ключевые слова. Генератор случайных чисел, микроконтроллер STM32, набор тестов NIST.

Генераторы случайных чисел (ГСЧ), используемые для криптографических приложений, обычно производят последовательности, состоящие из случайных битов нулей и единиц. Существует два основных класса ГСЧ: детерминированный ГСЧ или псевдослучайный и недетерминированный ГСЧ или истинный.

Псевдослучайный ГСЧ состоит из алгоритма, который производит последовательность битов из начального значения, называемого зерном. Значения, производимые псевдослучайным ГСЧ, полностью предсказуемы, если известны зерно и алгоритм генерации, поэтому зерно должно храниться в секрете и генерироваться из истинного ГСЧ.

Истинный ГСЧ создает случайную последовательность, которая зависит от некоторого непредсказуемого физического источника (источника энтропии), не зависящего от воздействия человека.

В некоторых сериях семейства микроконтроллеров STM32 от производителя STMicroelectronics (серии F2, F4, F7, L0, L4, L4+, H7, L5) присутствует встроенный аппаратный модуль истинного ГСЧ.

Истинный ГСЧ, реализованный в микроконтроллерах STM32, основан на аналоговой схеме. Эта схема генерирует непрерывный аналоговый шум, который используется при работе модуля ГСЧ для получения 32-битного случайного числа. Схема состоит из нескольких кольцевых генераторов, выходы которых объединяются методом XOR. Работа ГСЧ синхронизируется специальным источником тактирования с постоянной частотой [1].

Для проверки ГСЧ используются как различные наборы тестов, анализирующие входную последовательность случайных чисел, такие как набор тестов NIST и Diehard, так и тесты, анализирующие сам источник энтропии [2].

В основе тестов NIST лежит понятие нулевой гипотезы, т.е. предположения, что между двумя фактами отсутствует какая-либо взаимосвязь. Существует также альтернативная гипотеза, которая опровергает нулевую гипотезу: т.е. между явлениями взаимосвязь существует. За нулевую гипотезу принимается предположение, что последовательность является истинно случайной, знаки которой появляются равновероятно и независимо друг от друга. Следовательно, если нулевая гипотеза верна, то генератор производит достаточно «хорошие» случайные числа.

Набор тестов NIST содержит в себе 15 тестов. Для тестирования с ГСЧ снимается некоторое число последовательностей заданной длины. 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. В ходе тестирования по каждому из тестов также проводится проверка доли последовательностей, прошедших статистический тест, и проверка однородности результатов тестирования путем определения распределения значений вероятности p [3].

Тестирование аппаратного модуля ГСЧ в составе микроконтроллера семейства STM32 проводилось с использованием отладочной платы STM32F4DISCOVER, которая собрана на основе микроконтроллера STM32F407VG, который имеет в своем составе аппаратный модуль истинного ГСЧ [4]. Для тестирования был собран макет, который состоит из отладочной платы STM32F4DISCOVER подключенной к персональному компьютеру с помощью преобразователя интерфейсов TTL-USB, который позволяет отладочной плате подключиться к виртуальному COM-порту персонального компьютера по интерфейсу USB. Микроконтроллер на отладочной плате с помощью модуля ГСЧ производит случайные слова размером 32 бит и передает их по последовательному интерфейсу UART на преобразователь интерфейсов, который ретранслирует полученные случайные слова в виртуальный COM-порт персонального компьютера, в котором полученные числа сохраняются с помощью приложения Терминал.

Тестирование ГСЧ микроконтроллера проводилось с использованием тестов NIST. Для этого с помощью макета было получено и протестировано 12 Мбайт случайных чисел. Результаты тестирования при заданном значении погрешности p=0,01 показаны в таблице 1.

Таблица 1 – Результаты тестирования аппаратного модуля ГСЧ в составе микроконтроллера STM32

№ п/п	Наименование теста	Результаты 1 (ST) (10x512000 бит)		пл))		Результаты 3 (пл) (100x1000000 бит)	
		P-VALUE	PROP	P-VALUE	PROP	P-VALUE	PROP
1	частотный побитовый тест	0.911413	1.000	0.739918	1.000	0.657933	0.990
2	частотный блочный тест	0.534146	1.000	0.122325	1.000	0.657933	1.000
3	тест кумулятивных сумм (ср)	0.436621	1.000	0.825665	1.000	0.508752	0.990
4	тест на последовательность одинаковых битов	0.739918	1.000	0.534146	1.000	0.816537	0.980
5	тест на самую длинную	0.534146	0.900	0.534146	1.000	0.616305	0.970

	последовательность единиц в блоке						
6	тест рангов бинарных матриц	0.739918	1.000	0.213309	1.000	0.616305	0.980
7	спектральный тест	0.534146	1.000	0.991468	0.900	0.171867	**0.910***
8	тест на совпадение неперекрывающихся шаблонов (ср)	0.554145	1.000	0.499111	0.977	0.496918	0.982
9	тест на совпадение перекрывающихся шаблонов	0.739918	1.000	0.350485	1.000	0.798139	1.000
10	универсальный статистический тест Маурера	0.739918	1.000	0.066882	1.000	0.066882	1.000
11	тест приблизительной энтропии	0.350485	1.000	0.066882	**0.700***	**0.000070***	**0.890***
12	тест на произвольные отклонения (ср)	-	1.000	-	1.000	0.469837	0.982
13	другой тест на произвольные отклонения (ср)	-	1.000	-	1.000	0.403517	0.995
14	тест на периодичность (ср)	0.442315	1.000	0.000319	**0.550***	**0.000000***	**0.735***
15	тест на линейную сложность	0.534146	1.000	0.911413	1.000	0.262249	0.990

В таблице указаны наименования тестов, результаты проверки распределения однородности последовательностей (P-VALUE) и результаты проверки доли прошедших тест последовательностей (PROP). В таблице представлены три набора результатов: результаты тестирования выборки размером 10 последовательностей по 512000 бит, приведенные производителем микроконтроллера (Результаты 1) [1], результаты тестирования такой же выборки, полученные с помощью отладочной платы (Результаты 2) и результаты тестирования с большей выборкой: 100 последовательностей по 1000000 бит (в соответствии с рекомендациями NIST [3]), полученные с помощью отладочной платы (Результаты 3).

Для некоторых тестов, в которых проводится несколько серий тестирования, результаты указаны как среднее арифметическое результатов каждого из тестирования. Так же для некоторых тестов результат не удалось получить из-за маленькой выборки.

Для выборки в 10 и 100 последовательностей при заданном значении погрешности p=0,01 значение PROP должно быть в пределах 0,895 .. 1 и 0,960 .. 1 соответственно, а P-VALUE должно быть ≥ 0.0001 независимо от количества последовательностей [3]. Результаты выходящие за рамки допустимых отмечены «*».

Как видно из результатов, реальные характеристики ГСЧ в составе микроконтроллера немного хуже заявленных производителем, однако большинство тестов были успешно пройдены даже при увеличенной выборке, что говорит о возможности использовать ГСЧ в составе микроконтроллера во многих применениях.

Список использованных источников:

1. AN4230 STM32 microcontroller random number generation validation using the NIST statistical test suite: Application note. - STMicroelectronics, 2010. – 27 p.

2. Herrero-Collantes, M. Quantum Random Number Generators / M. T. Crane // Reviews of Modern Physics. – 2017. – №89(1). – 54 p.

3. A Statistical Test Suitefor Random and Pseudorandom Number Generators for Cryptographic Applications. – National Institute of Standards and Technology, 2010. – 131 p.

4. UM1472 Discovery kit with STM32F407VG MCU: User manual. - STMicroelectronics, 2020. – 32 p.