ВЛИЯНИЕ ДЛИТЕЛЬНОСТИ РАБОТЫ КОЛЬЦЕВОГО ОСЦИЛЛЯТОРА НА СТАТИСТИЧЕСКИЕ ХАРАКТЕРИСТИКИ ПОСЛЕДОВАТЕЛЬНОСТИ БИТ, СГЕНЕРИРОВАННОЙ АППАРАТНЫМ ГЕНЕРАТОРОМ СЛУЧАЙНЫХ ЧИСЕЛ

Кохновский С. И., Иванюк А. А
Кафедра информатики, Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: stan.ver.i.esk.slav@gmail.com, ivaniuk@bsuir.by

В данной работе описано влияние длительности работы кольцевого осциллятора на статистические характеристики последовательности бит, сгенерированной аппаратным генератором случайных чисел реализованным на плате FPGA Digilent Nexys 4.

Введение

В настоящее время существует достаточно широкий спектр аппаратных генераторов случайных чисел. Однако несмотря на высокие статистические показатели, известные генераторы обладают и существенным недостатком – высокой аппаратной сложностью. Данный недостаток критичен при применении генераторов в проектах с значительными ограничениями в ресурсах. Решением проблемы является использование относительно простой системы, удовлетворяющей заданному порогу качества.

I. Описание структуры генератора случайных чисел

Архитектурно компонент реализован на основе D-триггера, где бит данных (D) соединён с битом выхода (Q) линией с инвертором. Данная конфигурация, представляющая собой комбинацию триггера и кольцевого осциллятора, может использоваться как аппаратный генератор случайных чисел, так как наличие кольцевого осциллятора способствует вводу триггера в метастабильное состояние (см. рис. 1).

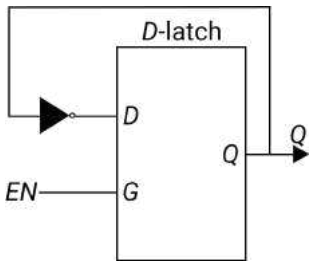

Рис. 1 – Логический компонент аппаратного генератора случайных чисел

Однако вход системы в метастабильное состояние занимает некоторое время после установки сигнала EN в логическую единицу, а сгенерированные значения не всегда являются статистически случайными из-за влияния большого количества иных факторов (смещения фазы, всевозможных задержек, аппаратных особенностей реализации FPGA и др.). В данной работе рассмотрено влияние продолжительности подачи сигнала EN триггеру на характеристики сгенерированной последовательности бит.

Для более наглядной демонстрации поведения системы реализован IP-компонент, состоящий из $num\_gen = 32$ описанных выше генераторов случайных чисел, а также содержащий логику управления длительностью передачи сигнала EN на вход генераторов, причём длительность передачи кратна длительности периода сигнала синхронизации системы. Сигнал EN подаётся на вход всем генераторам чисел в течение равного количества периодов синхронизации. В качестве управляющего компонента выбран процессор microblaze, сконфигурированный для работы на частоте 100 MHz.

II. Описание эксперимента

Эксперимент состоит в получении и исследовании характеристик сгенерированных последовательностей. Длины сгенерированных каждым из num_gen генераторов последовательностей составили 1000 бит. Обозначим количество единиц, сгенерированное генератором под номером i, как num_ones_i, тогда количество единиц, сгенерированное всеми генераторами, равно $num\_ones = \sum_{i=1}^{num\_gen} num\_ones_i$. Аналогично, для общего количества сгенерированных чисел используем обозначение $len = \sum_{i=1}^{num\_gen} len_i$, где количество сгенерированных символов генератором i обозначим len_i. Также введём обозначение для среднего арифметического сгенерированных символов: $mean = \frac{num\_ones}{len}$. При продолжительности установки бита $EN = 1$ в $k = 1$ период сигнала синхронизации большая часть генераторов возвращает одно и то же значение - 0 (см. рис. 2). На рисунке зелёным цветом выделен график $y = 0.5$ (половина сгенерированных символов - 1). Красным цветом обозначен график $y = mean$. Из информации на графике можно сделать вывод, что процент единиц от общего количества сгенерированных символов не достигает 12%.

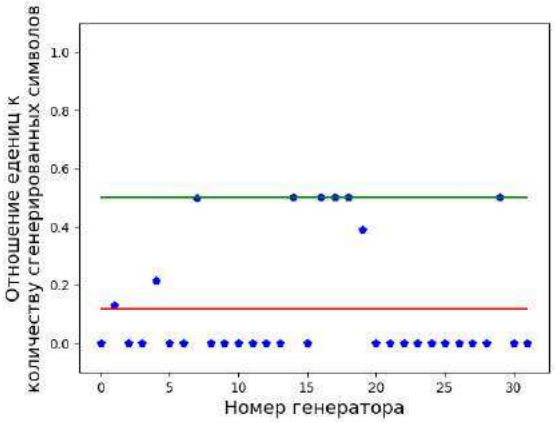

Рис. 2 – Отношение количества единиц к количеству сгенерированных символов для num_gen генераторов при подаче сигнала EN в течение $k = 1$ периода сигнала синхронизации

При увеличении времени удержания сигнала EN в единице до 8 периодов сигнала синхронизации увеличился разброс измерений, а значение $mean$ приблизилось к 0.5 (см. рис. 3), что свидетельствует о более случайной природе работы генераторов, впрочем, о статистической случайности речи не идёт - num_ones остаётся на отметке менее 34% от количества всех сгенерированных символов, а половина генераторов генерируют последовательности с сильным преобладанием нулей или единиц.

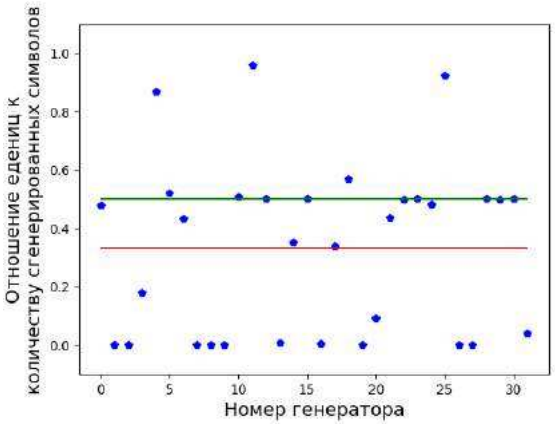

Рис. 3 – Отношение количества единиц к количеству сгенерированных символов для num_gen генераторов при подаче сигнала EN в течение $k = 8$ периодов сигнала синхронизации

При дальнейшем увеличении времени подачи сигнала EN до 1024 циклов сигнала синхронизации соотношение $mean$ стало ближе к 0.5, в то время как на всём множестве генераторов наблюдается выравнивание значений num_ones_i за исключением редких выбросов, частота появления которых также уменьшается по мере увеличения времени генерации (см. рис. 4).

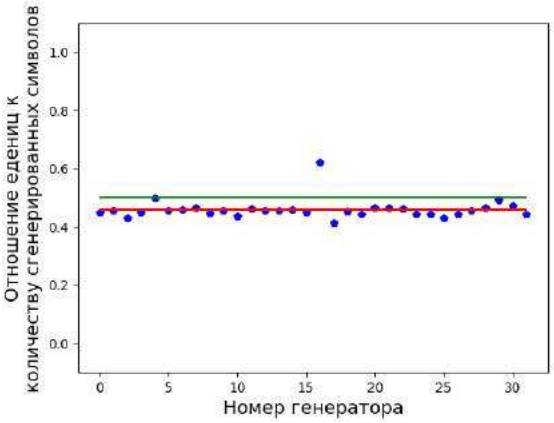

Рис. 4 – Отношение количества единиц к количеству сгенерированных символов для num_gen генераторов при подаче сигнала EN в течение $k = 1024$ периодов сигнала синхронизации

Рассмотрим диапазоны, в которые попадают измерения на всех генераторах с увеличением времени генерации (таблица 1). Из-за высокого количества нулей при $k < 8$ дальность разброса измерений относительно невысока (около 0.5), однако после $k = 4$ диапазон значений становится близок к единице, но с значения $k = 8$ начинает убывать.

Таблица 1 – Начало и ширина диапазона, в который попадают значения $\frac{num\_ones_i}{len_i}$, $i = \overline{1, num\_gen}$

	k					
	1	8	64	256	1024	65536
от	0.0	0.0	0.2	0.427	0.415	0.405
диап.	0.5	0.96	0.449	0.15	0.205	0.086

Выводы

Проведённое исследование позволяет сделать следующие выводы:

- при увеличении продолжительности подачи сигнала $EN = 1$ на вход генератора числовой последовательности, улучшаются статистические показатели сгенерированной последовательности, такие как приближение доли единиц к 0.5, выравнивание доли нулей и единиц в блоках поизвольной длинны, а также длительностей монотонного генерирования 0 или 1;
- наиболее быстрое уравнивание количества единиц в каждой из сгенерированных последовательностей происходит быстрее всего после $k = 8$, но при приближении к $k = 256$ улучшение показателей заметно не столь ярко.

Список литературы

1. An Area Efficient True Random Number Generator Based on Modified Ring Oscillators [Electronic resource] / Mehmet Alp Şarkışla, Salih Ergün. – Institute of Electrical and Electronics Engineers, 2018. – Mode of access: https://ieeexplore.ieee.org/document/8605697. – Date of access: 20.10.2021.