СХЕМА ПОСТОБРАБОТКИ ЦИФРОВОЙ ПОСЛЕДОВАТЕЛЬНОСТИ СЛУЧАЙНЫХ ЧИСЕЛ

Петровский Д.А.

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

Иванюк А.А. – докт. тех. наук

В данной работе рассмотрен процесс проектирования схемы постобработки последовательности случайных чисел на базе многоканального сигнатурного анализатора, приведен результат первичной оценки обработанной последовательности с использованием графических тестов и расчета энтропии по Шеннону.

Источником случайных чисел в цифровых системах является такой модуль как True Random Number Generator (TRNG). Способ сбора энтропии и превращения ее в поток битов является основой TRNG. Эта часть TRNG называется источником энтропии. Для этой цели могут использоваться различные физические принципы. Существует большое количество различных типов сбора энтропии, каждый из которых имеет свои достоинства и недостатки. Однако одним из основных отличий является то, основан ли источник энтропии на аналоговой или цифровой схемотехнике. Когда источник основан на аналоговой схемотехнике возникает потребность в использование АЦП. В том случае, когда источник энтропии основан на цифровой схемотехнике АЦП не требуется. В качестве примера можно привести источник, основанный на физически неклонируемой функции (ФНФ).

Сфера применения случайных чисел велика, они используются в криптографии, статистике, игровой индустрии, моделировании и т.д. Для каждой области существуют свои требования к качеству случайных чисел, их распределению и времени генерации. Существует множество стандартов, описывающих не только характеристики, но и предлагающих ряд тестов, прохождение которых обеспечит соответствие тому или иному стандарту. Каждый из стандартов описывает свою область применения случайных числе и может быть обязателен для того или иного региона. В качестве примера можно привести стандарты SP 800-90A-D и ряд из 15 тестов Национального института стандартов и технологий США (анг. National Institute of Standards and Technology (NIST), USA).

Однако, хочется отметить, что источники энтропии могут обладать далеко не самыми лучшими статистическими показателями. Для улучшения характеристик и приведения распределения к требуемому используют блок постобработки. В частности, для задач криптографии необходимо равномерное распределение случайных величин. Существует множество подходов, в качестве примера будут приведены следующие. Первый, использование одноканального сигнатурного анализатора (ОСА) для обработки последовательности бит, данный ОСА устанавливается на каждый канал (источник энтропии). Недостатком этого подхода является масштабируемость, так как для каждого канала необходимо использовать свой анализатор. Второй подход заключается в использовании сдвигового регистра с линейной обратной связью (анг. linear feedback shift register, LFSR) в режиме генератора, для последующего гаммирования с символами каналов (источников энтропии). Недостаток этого подхода – не самые лучшие статистические показатели.

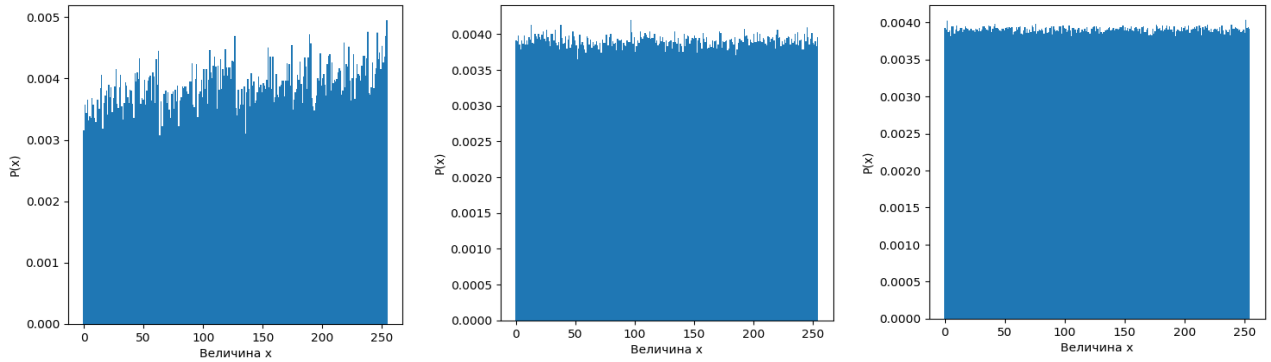
В данной работе предлагается использовать многоканальный сигнатурный анализатор (МСА), реализующий сжатие во времени. Под сжатием во времени понимается выполнение нескольких тактов работы устройства за один. Тем самым предполагается увеличение количества выходных каналов по сравнению со входным.

В научной работе [2], приведена методика проектирования МСА с количеством входов n и количеством выходов m, который эквивалентен ОСА длины m с последовательным мультиплексированием n каналов в один. Таким образом, МСА состоит из регистра, блока линейной обратной связи и блока коммутации входных каналов. Блок линейной обратной связи, функционально похож на схему формирования обратной связи в LFSR, но вычисляется значение не одного, а k бит, при $n \leq m$, $k = n$, *при* $n>m$ произойдет изменение всех выходных битов, $k = m$. Таким образом можно реализовать прыжок по орбите LFSR. Блок коммутации входных каналов распределяет их в зависимости от заданного полинома по соответствующим разрядам. После чего вычисляется побитовое «исключающее или» выходов обоих блоков и записывается в регистр.

Для реализации сжатия во времени МСА введем J – коэффициент сжатия во времени (количество тактов МСА, выполненных за один). Так как все операции, используемые в МСА, являются ассоциативными, то можно рассматривать блоки отдельно. Применительно к блоку линейной обратной связи, произойдет следующее изменение, количество вычисляемых бит увеличится в J раз. Касательно функции блока коммутации, то он будет итеративно применен J раз ко входным данным, тем самым обеспечивая распространение входной энтропии по всем выходным разрядам.

В данной работе оценивается равномерность распределения вероятностей случайной величины с помощью графического теста, а также изменение энтропии по Шеннону в зависимости от J. В качестве исходной последовательности был взят набор данных, сгенерированных с схемотехнической

реализации ФНФ [3], плотность распределения вероятностей данной последовательности представлена на рисунке 1а. Распределение экспериментальных данных подтверждает необходимость использования постобработки для достижения равномерного распределения. На рисунке 1б представлен результат обработки тесового набора МСА, с использованием примитивного полинома 32 степени с коэффициентом сжатия $J = 1$. На рисунке 1в представлен результат обработки той же последовательности МСА с аналогичным полиномом, но коэффициентом сжатия $J = 31$.



а) б) в)

Рисунок 1 – Плотность вероятностей а) исходного набора б) МСА с коэффициентом сжатия $J = 1$

в) МСА с коэффициентом сжатия $J = 31$

В качестве первичной математической оценки была рассчитана энтропия по Шеннону. На рисунке 2 представлены графики изменения энтропии в зависимости от величины коэффициента сжатия J для 4 различных примитивных полиномов 32 степени. Видно, что до определенного момента значение энтропии возрастает, а при значении J > 12 выходит на стабильный уровень с незначительными девиациями относительно величины 0.9999915. Это связано с распространением влияний входных каналов на весь сигнатурный анализатор.

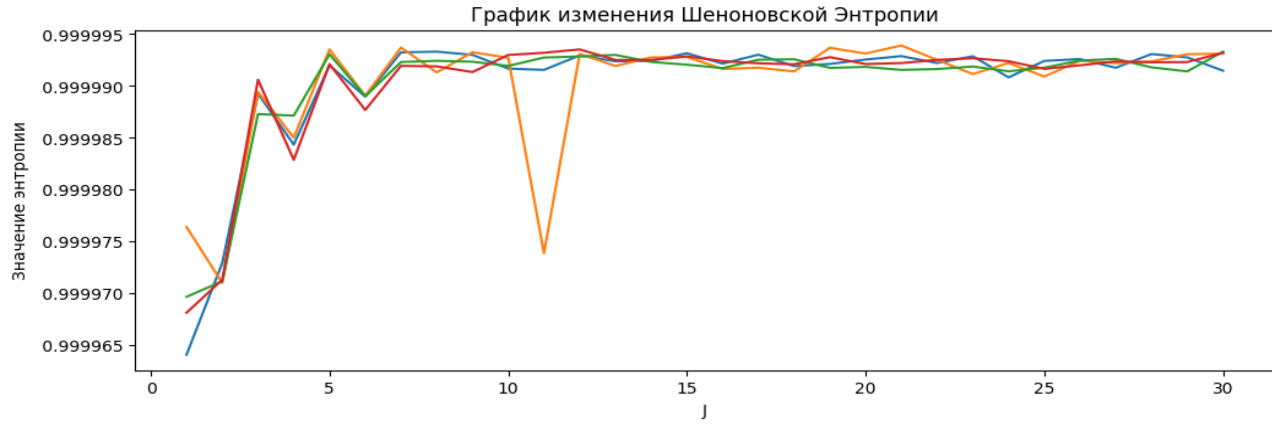


Рисунок 2 – Изменения значения энтропии в зависимости от J

В результате проектирования схемы постобработки последовательности случайных чисел была получена математическая модель, описывающая её. В процессе оценки результатов было получено распределение близкое к равномерному с максимальным значением энтропии по Шеннону 0.999994. Для развития данной идеи в дальнейшем планируется расширить анализ выходных данных устройства с использованием набора тестов предлагаемых NIST. Также нахождение зависимостей численного значения энтропии от полиномов и коэффициента сжатия $J > m$.

Список использованных источников:

1. Национальный институт стандартов и технологий США [Электронный ресурс] – режим доступа https://www.nist.gov/

2. В. Н. Ярмолик, “Построение многоканальных сигнатурных анализаторов”, Автомат. и телемех., 1985, № 1, 127–132

3. Шамына А.Ю., Иванюк А.А. Исследование временных параметров физически неклонируемой функции типа арбитр с использованием кольцевого осциллятора. Цифровая трансформация. 2022;28(1):27-38