ИНФОРМАТИКА

УДК 004.353.2

ОЦЕНКА КАЧЕСТВА ПРОСТОГО АППАРАТНОГО ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ

П.Л. Чечет, В.Д. Левчук, А.В. Воруев, Е.А. Левчук

Гомельский государственный университет им. Ф. Скорины

ESTIMATION OF QUALITY OF SIMPLE HARDWARE RANDOM NUMBERS GENERATOR

P.L. Chechat, V.D. Liauchuk, A.V. Varuyeu, A.A. Liauchuk

F. Scorina Gomel State University

Предлагается простая реализация аппаратного генератора случайных чисел, использующего эффект лавинного пробоя перехода биполярного транзистора. По результатам статистических экспериментов сделан вывод о возможности использования данного устройства в различных аппаратно-программных комплексах.

***Ключевые слова**: аппаратный генератор случайных чисел, генератора шума, лавинный пробой перехода транзистора, статистический критерий.*

A simple implementation of a hardware random number generator that uses the avalanche breakdown effect of the bipolar transistor transition is offered. According to the results of statistical experiments, a conclusion is made about the possibility of using this device in various hardware-software systems.

***Keywords**: hardware random numbers generator, noise generator, avalanche breakdown of a transistor, statistical criterion.*

Введение

Вопросы получения псевдослучайных последовательностей, во многом успешно решённые ещё в прошлом веке, в настоящее время снова получили актуальность в связи с широким распространением мобильных вычислительных устройств. С одной стороны, их постоянное повышение производительности позволяет использовать все те алгоритмы и приёмы для получения псевдослучайных последовательностей, что и на стационарных компьютерах. С другой стороны, вопросы снижения стоимости аппаратной части, её упрощения, всё равно остаются актуальными, так как это напрямую влияет на себестоимость устройства, его энергопотребление. А именно эти вопросы всегда являются важными для производителей.

В свете вышесказанного имеются приложения, где есть смысл в использовании не программных генераторов псевдослучайных чисел, а аппаратных датчиков случайных чисел. Использование аппаратных датчиков случайных числовых последовательностей позволяет получить действительно случайную последовательность, которую невозможно предсказать, что недостижимо при использовании псевдослучайных последовательностей. Это может быть критично, например, в мобильных приложениях, использующих шифрование.

1 Выбор аппаратного датчика случайных чисел

Известно, что в качестве аппаратного датчика случайных чисел можно взять практически любой стохастический процесс и организовать из него выборку значений. В устройствах, требующих наглядности (лотереи, розыгрыши), широко используются механические или электромеханические устройства. В цифровых устройствах по понятным причинам (размеры, быстродействие, энергопотребление) целесообразно использовать чисто электронные датчики случайных чисел. Наиболее популярным вариантом являются различные варианты схем генераторов шума [1].

В качестве исследования был выбран один из самых простых вариантов схемы генератора шума, основанный на лавинном пробое перехода транзистора. Для сопряжения его с компьютером и передачи получаемых значений было задействовано устройство, описанное в [2]. Упрощённо схема генератора шума и части устройства, обеспечивающего интерфейс взаимодействия, приведена на рисунке 1.1.

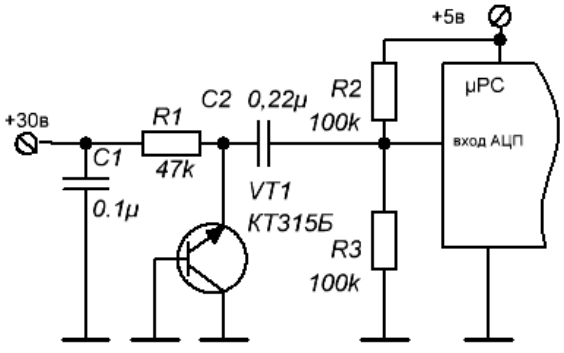

Рисунок 1.1 – Упрощённая схема датчика чисел

Из рисунка видно, что на вход аналого-цифрового преобразователя (АЦП) микроконтроллера через делитель на резисторах R2 и R3 поступает половина напряжения питания. Поступающий шумовой сигнал вызывает смещение этого напряжения в сторону увеличения или уменьшения. Сопротивления резисторов R2 и R3 выбраны таким образом, что амплитуда шума не превышает 2.5 вольта, что позволяет избежать ограничений по измерению напряжения АЦП микроконтроллера. Опорное напряжение для АЦП программно сконфигурировано равным напряжению питания – 5 вольт.

АЦП большинства недорогих микроконтроллеров Atmel семейства AVR имеет 10 разрядов, что позволяет получать значения в диапазоне от 0 до 1023. Поступаемое на вход АЦП напряжение измеряется через постоянные интервалы времени, полученные значения передаются в программу на компьютере через последовательный интерфейс. Подробно этот процесс передачи данных описан в [2].

Так как амплитуда измеряемых значений не превышает 2.5 вольт, значения от АЦП не достигают крайних значений 0 и 1023. Для корректного применения критериев проверки качества полученной случайной последовательности был выполнен её сдвиг на величину минимального полученного значения, равного по результатам измерений 21. Что позволило в итоге получать значения в диапазоне от 0 до 981. Для проверки корректности выбора диапазонов значений использовался запуск устройства на продолжительное время (несколько часов) с сохранением в программе экстремальных значений (максимума и минимума) и дальнейшей передачей их в персональный компьютер.

2 Анализ распределения полученных значений

Для определения закона распределения случайной величины, значения которой возвращает выбранный аппаратный датчик случайных чисел, была построена гистограмма распределения частот для десяти равных отрезков. Частоты распределения 2 000 сгенерированных значений по отрезкам представлены на рисунке 2.1.

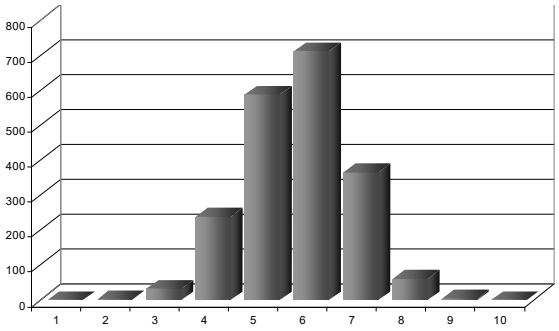

Рисунок 2.1 – Гистограмма распределения частот

Визуально по гистограмме можно предположить, что выборка значений, полученных от аппаратного датчика случайных чисел, имеет нормальное распределение. Среднее значение по выборке равно 506,6. Оценка дисперсии – 10 329,7. Распределение эмпирически полученных значений и теоретическое по отрезкам приведено в таблице 2.1.

Таблица 2.1 – Распределение значений по отрезкам

Отрезок	Эмпирическое значение	Теоретическое значение
1	0	0,1
2	2	2,2
3	32	34,7
4	239	225,9
5	587	615,2
6	711	705,6
7	465	341,1
8	60	69,2
9	4	5,8
10	0	0,2

Используя критерий χ^2 получаем значение 6,07, что меньше критического значения, равного 22,3 для уровня значимости 10%. Следовательно, выдвинутая гипотеза о нормальном распределении согласуется с экспериментальными данным.

Для дальнейшей проверки последовательности, полученной от аппаратного датчика случайных чисел, был применён критерий Колмогорова – Смирнова. Построенные по выборке эмпирическая и теоретическая функции распределения представлены на рисунке 2.2.

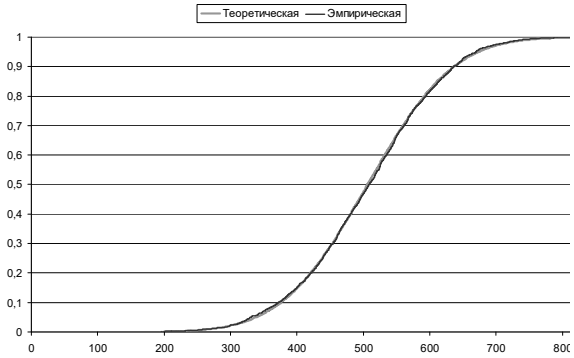

Рисунок 2.2 – График функций распределения

Значения статистик КС-критерия получились следующие:

$$K_n^+ = \sqrt{n} \max_{-\infty<x<+\infty} \left(F_n(x) - F(x)\right) \approx 0,50,$$
$$K_n^- = \sqrt{n} \max_{-\infty<x<+\infty} \left(F(x) - F_n(x)\right) \approx 0,71, \quad (2.1)$$

где $F(x)$ – теоретическая функция нормального распределения с заданными средним и среднеквадратичным отклонением, $F_n(x)$ – эмпирическая

функция распределения, построенная по выборочным значениям x_i:

$$F_n(x) = \frac{1}{n}\sum_{i=1}^{n}\begin{cases}1, & x_i < x;\\ 0, & x_i \geq x.\end{cases} \qquad (2.2)$$

Из (2.1) видно, что значения статистик меньше табличного (критического) для $n = 2\,000$, равного 1,36. Следовательно, гипотеза о нормальности распределения значений, получаемых с помощью выбранного аппаратного датчика, согласуется с экспериментальными данными.

Для проверки также был применён модифицированный вариант *критерия Шапиро – Уилка* [3], не требующий таблиц, так как $n = 2\,000$. Отсутствие таблиц не освобождает от необходимости вычислять коэффициенты a_j:

$$a_0 = \frac{0.899}{(n-2,4)^{0.4162}} - 0.02,$$

$$a_j = a_0\left[z + \frac{1483}{(3-z)^{10.845}} + \frac{71.6\cdot 10^{-10}}{(1.1-z)^{8.26}}\right],$$

$$z = \frac{n-2j+1}{n-0.5}. \qquad (2.3)$$

Поэтому коэффициенты a_j были вычислены программно по формулам (2.3). Далее по известной формуле из [3] было вычислено критическое значение W_1 для уровня значимости $\alpha = 0.05$.

$$W_1 = \left(1 - \frac{0.6695}{n^{0.6518}}\right)\frac{s^2}{B},$$

$$B = \left[\sum_{j=1}^{n/2} a_j (x_{n-j+1} - x_j)\right]^2,$$

где s^2 – дисперсия рассматриваемой случайной величины.

Вычисление всех выражений было реализовано программно, по результатам работы значение статистики $W_1 \approx 2.22$, что больше критического значения, равного единице. Следовательно, гипотеза согласуется с экспериментальными данными.

Заключение

Аппаратные датчики случайных чисел при своих недостатках (размеры, энергопотребление, невозможность воспроизведения) позволяют, в отличие от датчиков псевдослучайных чисел, получать действительно случайные числовые последовательности. Есть приложения, где это условие является критическим. Это, например, реализация различных лотерей, генерация случайных ключей для шифрования данных. В данной статье рассмотрен один из простейших вариантов реализации аппаратного датчика случайных чисел, использующего эффект лавинного пробоя перехода биполярного транзистора. Оказалось, что значения, получаемые с помощью этого датчика, можно считать нормально распределёнными и использовать их для соответствующих применений. Данный факт был проверен и подтверждён с помощью нескольких статистических критериев. Простота технической реализации и невысокие требования к микроконтроллеру устройства (современные модели практически всегда имеют встроенный аналого-цифровой преобразователь) позволяют использовать подобные аппаратные датчики случайных чисел во многих устройствах, как стационарных, так и переносных и носимых. Например, в популярных сегодня проектах на Arduino.

ЛИТЕРАТУРА

1. *Простая схема генератора шума*. – Режим доступа: http://sxtmns1.appspot.com/prostaya-shema-generatora-shuma.html. – Дата доступа: 02.10.2015.

2. *Чечет*, П.Л. Разработка интерфейса взаимодействия электронного устройства с компьютером / П.Л. Чечет // Известия Гомельского государственного университета им. Ф. Скорины. – 2011. – № 6 (69). – С. 200–203.

3. Критерий Шапиро – Уилка. – Режим доступа: www.machinelearning.ru/wiki/index.php?title=Критерий_Шапиро-Уилка. – Дата доступа: 30.12.2015.

Поступила в редакцию 16.03.18.