Исследование вероятностных характеристик генератора действительно случайных числовых последовательностей на основе физически неклонируемых функций

Заливако С.С.; Иванюк А.А.
Кафедра вычислительных методов и программирования
Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
e-mail: zalivako@mail.ru, ivaniuk@bsuir.by

***Аннотация*—Данная статья посвящена исследованию генератора действительно случайных числовых последовательностей. В основе работы генератора лежат цифровые реализации физически неклонируемых функций. Произведено тестирование последовательностей, которые вырабатывает генератор при помощи пакета статистических тестов NIST.**

Ключевые слова: генератор действительно случайных числовых последовательностей; физически неклонируемые функции; статистические тесты NIST

I. Введение

Последовательность случайных чисел является одним из ключевых элементов целого ряда прикладных задач из областей криптографии, моделирования, игровой индустрии (компьютерные игры, азартные игры, лотереи и т.п.), квантования, принятия решений, искусства [1].

По сравнению с генераторами псевдослучайных числовых последовательностей они обладают следующими преимущества и недостатками (табл. 1):

Табл. 1. Преимущества и недостатки генераторов действительно случайных чисел

Преимущества	***Недостатки***
Непериодичность, непредсказуемость	Медленный и неэффективный
Нет зависимостей между элементами последовательности	Сложность запуска и установки
Высокий уровень безопасности	Дороговизна изготовления
Не основаны на алгоритмах	Имеются возможности вредоносного воздействия

II. Теоретическое обоснование работы генератора

В основе идеи генерирования случайных чисел лежат реализации физически неклонируемых функций (ФНФ), которые, в свою очередь, являются функциями «извлечения» структурных неоднородностей кристаллов интегральных схем.

Гипотеза данной работы состоит в том, что генератор случайных чисел (ГСЧ), построенный на основе ФНФ, будет являться невоспроизводимым и неклонируемым цифровым устройством.

За основу схемной реализации ГСЧ возьмем ФНФ типа «кольцевой генератор» (RO-PUF, Ring Oscillator Physical Unclonable Function). Аппаратная схема ФНФ типа RO может быть реализована с помощью n пар инверторов и мультиплексора [2].

Теоретически совместная работа двух элементов типа RO-PUF на одном диапазоне частот и с разным количеством инверторов (параметр n) позволит получать действительно случайную последовательность битов, которая в дальнейшем будет взята за основу окончательной случайной последовательности.

Поскольку реализации ФНФ в действительности имеют различные характеристики и могут быть реализованы на разных кристаллах, то генерируемая последовательность будет невоспроизводима, непериодична, непредсказуема.

III. Реализация схемы генератора

Схема генератора действительно случайных числовых последовательностей представляет генератор тактовых импульсов с частотой 50 МГц, генератор одиночного импульса скважностью X, двух элементов RO-PUF, сумматора по модулю 2, сдвигового регистра с линейной обратной связью (LFSR, Linear feedback shift register) [3] (см. рис. 1).

Исследование показало, что с увеличением периода работы генератора одиночного импульса улучшаются статистические свойства генерируемой последовательности. На малых значениях периода возможно решение задачи идентификации схемы.

Сгенерированный импульс в определенной полосе пропускания дает возможность элементам, реализующим ФНФ, вырабатывать значения битов, которые поступают на вход сумматора по модулю два. На выходе же сумматора формируется последовательность битов, которая поступает на вход сдвигового регистр с линейной обратной связью, который, в свою очередь, сжимает данную последовательность битов, т.е. служит одноканальным сигнатурным анализатором, что придает ей равномерное статистическое распределение.

IV. Тестирование генератора

Пакет статистических тестов NIST включает в себя 15 тестов, которые необходимы для проверки случайности бинарной последовательности, сгенерированной аппаратным или программным генератором последовательности случайных

(псевдослучайных) чисел. Главное, что показывает результат работы данного пакета – это наличие ряда элементов неслучайности в последовательности [3].

Опишем результаты тестирования (проведено 13 тестов) последовательности, выработанной генератором:

Табл. 2. РЕЗУЛЬТАТ ТЕСТИРОВАНИЯ ПОСЛЕДОВАТЕЛЬНОСТИ

Статистический тест	***P-значение***	***Пройден ли тест***
Частотный тест	0.350485	Да
Частотный блочный тест	0.534146	Да
Тест на последовательность одинаковых бит	0.122325	Да
Тест на самую длинную последовательность единиц в блоке	0.534146	Да
Тест рангов бинарных матриц	0.350485	Да
Спектральный тест	0.350485	Да
Тест неперекрывающихся шаблонов	0.350485	Да
Тест перекрывающихся шаблонов	0.534146	Да
Универсальный статистический тест Маурера	0.000000	Нет
Тест на линейную сложность	0.534146	Да
Тест на периодичность	0.739918	Да
Тест приблизительной энтропии	0.000000	Нет
Тест куммулятивных сумм	0.213309	Да

Как видно из таблицы, последовательность, которая была сгенерирована, обладает хорошими статистическими свойствами, поскольку 11 тестов из 13 были успешно пройдены.

Критичным является, что тест Маурера (на возможность сжатия последовательности) не проходит, а также последовательность не обладает таким же уровнем энтропии, как истинно случайная (эталонная) последовательность случайных чисел.

Перечисленные выше статистические недостатки случайной последовательности могут быть преодолены, например, изменением (увеличением) скважности одиночного импульса, а также увеличением разрядности LFSR.

V. ВЫВОДЫ И ПЕРСПЕКТИВЫ

Данный генератор обладает рядом преимуществ:

- нетрудоемкость изготовления (количество используемых для реализации элементов мало по сравнению с другими реализациями [5, 6]);
- генерируемая последовательность обладает хорошими статистическими свойствами (свойства неклонируемости и невоспроизводимости были проверены на двух идентичных ПЛИС);

Однако генератор несет в себе и определенные недостатки:

- сгенерированная последовательность не проходит тест на сжимаемость и энтропию, что отрицательно сказывается на случайности данной последовательности;

Данный генератор, как уже отмечалось выше, может быть использован для решения задачи идентификации.

[1] K. Charmaine “Random number generators: An evolution an comparison of Random.org and some Commonly used Generators”, Management Science and Information Systems Studies. Project Report, pp. 6–10, April 2005.

[2] Иванюк, А. А. Проектирование встраиваемых цифровых устройств и систем: монография / А. А. Иванюк. - Минск: Бестпринт, 2012, с. 285-294.

[3] Ярмолик, В. Н., Демиденко, С. Н. Генерирование и применение псевдослучайных сигналов в системах испытания и контроля / В. Н. Ярмолик, С. Н. Демиденко. – Минск : Наука и техника, 1986, с. 80 – 100.

[4] “A Statistical Test Suite for Random and Pseudorandom Number Generators for Criptographic Application” / Andrew Rukhin and other. NIST special publication, pp. 271–350, April 2010.

[5] A. Maiti, R. Nagesh, A. Reddy, P. Schaumont, "Physical Unclonable Function and True Random Number Generator: a Compact and Scalable Implementation," 19th Great Lakes Symposium on VLSI (GLSVLSI 2009), May 2009.

[6] A. Sadr, M. Zolfaghary-Nejad “Physical Unclonable Functions (PUF) Based Random Number Generator”, Advanced Computing: An International Journal (ACIJ), Vol.3, No.2, March 2012

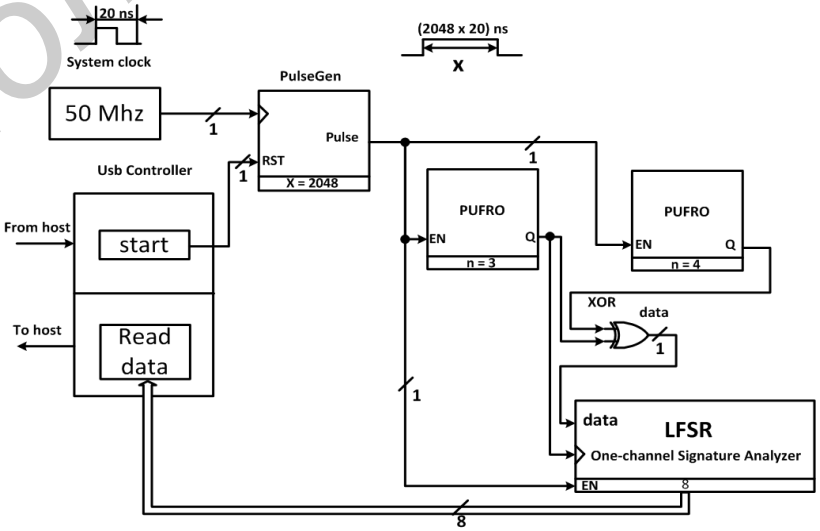

Рис. 1. Схема генератора