ГЕНЕРИРОВАНИЕ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЕЙСТВИТЕЛЬНО СЛУЧАЙНЫХ ЧИСЕЛ С ПОМОЩЬЮ ФИЗИЧЕСКИ НЕКЛОНИРУЕМОЙ ФУНКЦИИ ТИПА АРБИТР

Заливако С. С., Иванюк А. А.
Кафедра вычислительных методов и программирования, кафедра информатики, Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: {zalivako, ivaniuk}@bsuir.by

Исследована возможность решения задачи генерирования действительно случайных числовых последовательностей с помощью физически неклонируемой функции типа арбитр. Для сжатия полученной в результате работы арбитров последовательности использовался многоканальный LFSR. Проведено тестирование генерируемой последовательности с помощью пакетов Statistica, Nist, Diehard.

Введение

Последовательности действительно случайных чисел часто используются для решения различных задачи в таких областях как криптография, моделирование, игровая индустрия, системы поддержки принятия решений, случайная выборка, искусство и другие [1]. В общем случае генератор действительно случайных числовых последовательностей (ГДСЧП) состоит из трех компонентов: источника энтропии, схемы сжатия и регистра хранения случайного числа.

Основной гипотезой данного исследования является предположение о том, что параллельная работа нескольких физически неклонируемых функций (ФНФ) типа арбитр [2] может служить источником энтропии.

I. ФНФ типа арбитр

Основная идея реализации ФНФ типа арбитр состоит в построении двух топологически и функционально идентичных путей на одном кристалле интегральной схемы. Такие пути носят название «симметричные пути», и имеют очень близкие величины времени распространения сигналов по ним. Однако физически такие пути принципиально различны благодаря различию результирующих составляющих для каждого из них. Такое различие объясняется физическими вариациями технологического процесса изготовления цифрового устройства.

ФНФ типа арбитр можно реализовать с помощью генератора одиночного импульса PG, выходной импульс которого подается на вход компонента, состоящего из $2n$ мультиплексоров, на каждую пару которых подается селектирующий сигнал C_i $(0 \leq i \leq n\text{-}1)$. Совокупность сигналов C_i называют запросом. Результат работы двух «цепочек» мультиплексоров (S_1 и S_2) подаются на вход D-триггера, который в свою очередь, и является «арбитром», определяя, какой из сигналов пришел раньше. Если первым пришел сигнал S_1, то результатом будет 1, в противном случае 0.

Схемная реализация ФНФ типа арбитр приведена на рис. 1.

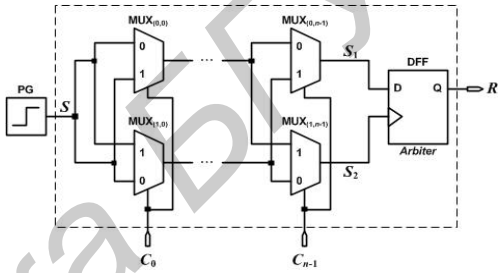

Рис. 1 – Схемная реализация ФНФ типа арбитр

Как показали эксперименты, результат работы ФНФ типа арбитр на одних и тех же запросах может незначительно варьироваться, что говорит о нестационарности этих откликов. Такие результаты позволили выдвинуть гипотезу о том, что несколько параллельно работающих ФНФ типа арбитр могут служить источником энтропии.

II. Реализация схемы генератора

Предлагаемый в данной работе генератор действительно случайных числовых последовательностей состоит из n параллельно работающих ФНФ типа арбитр и многоканального LFSR [3] в качестве схемы сжатия (см. рис. 2).

До применения схемы сжатия генерируемая последовательность обладала элементами случайности и, как следствие, не проходила большинство тестов NIST [4].

Аппаратурные затраты на реализацию генератора приведены в таблице 1.

Таблица 1 – Аппаратурные затраты на реализацию генератора

Разрядность случайного числа	Число LUT-блоков	Число триггеров (DFF)
2 бита	25 из 9312	8 из 9312
4 бита	55 из 9312	12 из 9312
8 бит	163 из 9312	20 из 9312

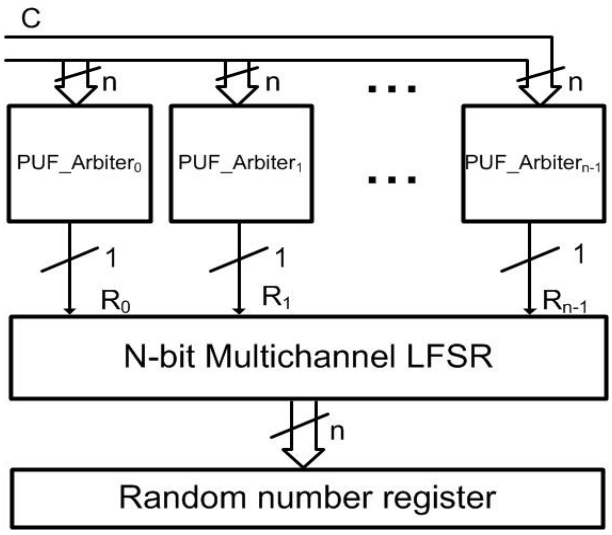

Рис. 2 – Структурная схема генератора

По сравнению с предыдущими работами авторов по реализации ГДСЧП на базе FPGA [5,6] аппаратурные затраты меньше в 4 раза по числу LUT-блоков и практически такие же по числу триггеров. Таким образом, данный генератор обеспечивает значительную экономию по количеству используемых блоков комбинационной логики.

III. Статистическое тестирование генератора

Результаты тестирования приведены в таблице 2.

Таблица 2 – Результаты тестирования генератора

Пакет тестирования	Описание тестов	Результат
Statistica	Проверка равномерности распределения, проверка корреляционной независимости выборок, генерируемых на разных платах	На уровне значимости α=0,5 принимается гипотеза о равномерности распределения генерируемой случайной последовательности, а также гипотеза о равенстве нулю коэффициента корреляции Пирсона
NIST	15 стандартных тестов NIST	на всех тестах процент выборок, прошедших тестирования превышает 95%
Diehard	15 стандартных тестов Diehard	На всех тестах p-значение больше 0,05, что говорит о положительном результате тестирования

Тестирование генератора было осуществлено на двух идентичных ПЛИС Xilinx Spartan 3E-500 FG320 с помощью пакета Statistica, пакета статистических тестов NIST и пакета статистических тестов Diehard.

Как видно из таблицы по результатам тестирования последовательности, вырабатываемые генератором, могут быть признаны действительно случайными.

IV. Преимущества и недостатки реализации

К преимуществам предлагаемой реализации можно отнести:

- простота изготовления;
- высокое качество генерируемой последовательности;
- последовательность обладает свойствами неклонируемости, невоспроизводимости;
- решение задачи генерирования случайных чисел совместно с решением задачи идентификации.

Предлагаемая реализация также обладает одним существенным недостатком – скорость генерирования последовательности достаточно мала (1,01 кБит/с);

В результате исследования удалось установить, что ФНФ типа арбитр, которую часто используют для решения задачи идентификации, может быть успешно использована в качестве источника энтропии с меньшими аппаратурными затратами по числу LUT-блоков более чем в 4 раза.

V. Список литературы

1. Charmaine, K. Random number generators: An evolution an comparison of Random.org and some Commonly used Generators, Management Science and Information Systems Studies. Project Report, April 2005.
2. A technique to build a secret key in integrated circuits for identification and authentification application / J. W. Lee [et al.] // VLSI Circuits: Proc. of Symp., Honolulu, Hawai, 17-19 Jun. 2004. – P. 176-159
3. Bardell, Paul H. Built In Test for VLSI: Pseudorandom Techniques / Paul H. Bardell, W. H. McAnney, J. Savir // New-York:Wiley-Interscience, 1987. – 448 p.
4. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Application / Andrew Rukhin and other. NIST special publication, April 2010.
5. Заливако, С. С. Исследование вероятностных характеристик генератора действительно случайных числовых последовательностей на основе физически неклонируемых функций / С. С. Заливако, А. А. Иванюк // Материалы международной научной конференции «ИТС 2012» – Минск: БГУИР, 2012. – с. 202-203.
6. Заливако, С. С. Использование физически неклонируемых функций для генерирования действительно случайных числовых последовательностей / С. С. Заливако, А. А. Иванюк // Автоматика и вычислительная техника. – 2013. – № 3. – С. 61–72.