Министерство Образования Республики Беларусь

Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.67

Ерминек
Катажина Ришардовна

Методы и алгоритмы синтеза цифровых генераторов случайных последовательностей

Автореферат
на соискание степени магистра технических наук
по специальности 1-40 80 01 «Элементы и устройства вычислительной техники и систем управления»

Научный руководитель

Иванюк Александр Александрович
д.т.н., профессор

Минск, 2015

Работа выполнена на кафедре электронных вычислительных средств учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель: **Иванюк Александр Александрович,** доктор технических наук, профессор кафедры информатики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Рецензент: **Лукьянец Владимир Григорьевич,** Кандидат технических наук, доцент кафедры экономической информатики учреждения образования «Минского государственного высшего радиотехнического колледжа»

Защита диссертации состоится «23» июня 2015 г. года в $11^{\underline{00}}$ часов на заседании Государственной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, г.Минск, ул. П.Бровки, 6, 1 уч корпуса.

ВВЕДЕНИЕ

В современных информационных технологиях активно используются действительно случайные числовые последовательности. Сферы их применения обширный : криптография, моделирование, игровая индустрия, системы поддержки принятия решений, случайная выборка.

В ***криптографии*** случайные числа применяются достаточно широко. Для сокрытия оригинальных данных необходимо создавать случайные шумы, для невозможности угадывания секретного ключа, который, как правило, является основой для алгоритма шифрования необходимо каким-то образом делать ключ непредсказуемым. Такая непредсказуемость и случайность может быть обеспечена за счет включения в криптосистему ГДСЧП.

В ***моделировании*** случайные числовые последовательности применяются для создания более реалистичных условий проведения опытных испытаний. Как правило, для осуществления какого-либо эксперимента в условиях, близких к реальным, необходимо воспроизведение каких-то случайных воздействий, которые имеют место в действительности. Использование ГДСЧП (возможно, числовая последовательность не будет использована в исходном виде, а будет преобразована к необходимому виду) как источника такого случайного воздействия является оправданным и нетрудоемким путем решения данной проблемы.

Существует множество способов получения случайных числовых последовательностей, однако они имеют множество недостатков:

— небольшая скорость генерирования случайных чисел;

— сложность запуска и установки;

— имеют аппаратные уязвимости;

— сложная процедура генерирования;

— требуются большие аппаратные и, соответственно, материальные затраты для изготовления;

— некоторые из них основаны на алгоритмах, т.е. потенциально могут быть предсказаны, поскольку этот алгоритм известен злоумышленником.

Для преодоления этих недостатков ГДСЧП необходимо реализовывать на базе FPGA, а в качестве источника случайности необходимо использовать физически неклонируемые функции, поскольку одним из основных свойств ФНФ является то, что пару запрос-отклик легко получить, но практически невозможно предсказать или же построить математическую модель, которая бы помогла это сделать; реализация ФНФ, как правило, не требует больших аппаратных затрат (требуется не более 4-5 логических элементов); устройство, реализованное на базе FPGA, может быть легко модифицировано, что ускоряет процесс разработки генератора.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

Необходимость предотвращения несанкционированных действий со стороны пользователей к получению информации является актуальной. Множество способов получения случайных числовых последовательностей обладают недостатками, выраженными в ограниченной скорости генерирования, аппаратной уязвимости, несанкционированном доступе к данным. Для преодоления данных недостатков необходима реализация задачи на базе FPGA. В качестве энтропии – источника случайности применены физически неклонируемые функции, результаты-отклики которых обладают непредсказуемостью, неклоруемостью, способностью к модификации. Для реализации актуальной задачи необходим анализ состояния области цифровых устройств, статистическое тестирование полученных последовательностей на предмет непредсказуемости.

Цель и задачи исследования

Для предотвращения несанкционированных действий со стороны пользователей к получению информации целью диссертации является разработка методики построения генератора случайных числовых последовательностей при помощи физически неклонируемых функций как источника энтропии.

Для выполнения и реализации поставленной цели были сформулированы следующие задачи:

— проанализировать существующее состояние области цифровых устройств, направленных на генерирование последовательности действительно случайных чисел;

— разработать методику генерирования действительно случайных числовых последовательностей;

— спроектировать цифровой генератор случайных чисел;

— реализовать спроектированный генератор на базе FPGA;

— разработать методику проведения эксперимента;

— провести эксперимент и проанализировать его результаты;

— произвести статистическое тестирование полученных последовательностей случайных чисел.

Теоретическая и методологическая основа исследования

В основу диссертации легли результаты известных исследований отечественных и зарубежных учёных в области криптографической защиты информации.

Для построения уникальных идентификаторов построения ПЛИС, а также проведения эксперимента разработано программное описание в виде VHDL-проекта, с дальнейшей модификации после проведения дополнительных экспериментов vhdl-описания. Использованы инструменты Digilent Adept 2, позволяющие программировать устройства ПЛИС Digilent (в том числе Basys2) файлами с расширением ".bit", сгенерированными средой Xilinx из программы на VHDL.

Все экспериментальные работы по исследованию свойств цифровых устройств проводились с применением макетных плат быстрого прототипирования Digilent NEXUS-2 с ПЛУ типа FPGA Xilinx SPARTAN XC3S500E, САПР цифровых устройств Xilinx ISE, системы моделирования ModelSim, и набора программных компонент Digilent Adept SDK.

Для проведения исследования взяты две идентичные системы B0 и B1 (Digilent Nexys-2 с ПЛИС FPGAXC3s500e-5FG320).

Теоретическая значимость диссертации заключается в анализе текущего состояния области генераторов действительно случайных числовых последовательностей. В качестве основы для проектирования ГДСЧП была взята стандартная структура, которая состоит из источника энтропии, схемы сжатия и регистра случайного числа. Реализации каждого из компонентов структуры были проанализированы на предмет преимуществ и недостатков, что помогло выбрать в качестве источника энтропии физически неклонируемые функции.

Практическая значимость диссертации заключается проведении экспериментов для процесса создания, тестирования и усовершенствования цифровых устройств, направленных на генерирование действительно случайных числовых последовательностей, а также реализованы цифровые устройства, усовершенствованные в результате проведения множества экспериментов и позволившие повысить качество генерируемой действительно случайной числовой последовательности, уменьшить аппаратные затраты на реализацию цифрового устройства.

.

Апробация практических результатов

Результаты исследования были представлены в республиканском конкурсе научных работ студентов и магистрантов, где отмечены 1 (2013 г.) и 2 категориями (2014 г.)

Основные результаты диссертации изложены в 3 опубликованных работах. Общее количество страниц опубликованных материалов – 10.

Структура и объем работы

Общий объем диссертационной работы составляет 61 страницы, включая библиографический список и приложение, текст содержит 15 рисунков. Структура диссертационной работы обусловлена целью, задачами и логикой исследования. Работа состоит из введения, трёх глав и заключения, библиографического списка и приложений.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** изложены актуальность темы исследования, основные направления в этой области, анализ и сравнение, отмечены преимущества и недостатки существующих методов, поставлены задачи исследования, определена сфера применения разработок.

В **первом разделе** произведен анализ генераторов действительно случайных последовательностей, представлена обобщенная структура, Описана необходимая методика коррекции получены значений.

Во **втором разделе** произведено теоретическое обоснование работоспособности генератора действительно случайных числовых последовательностей и физически неклонируемых функций как источника энтропии.

Третий раздел посвящен экспериментальному исследованию различных реализаций генераторов действительно случайных числовых последовательностей с указанием методики проведения, а также реализации эксперимента. Результаты представлены в виде графиков,сравнительных таблиц, результата синтеза программы.

В **приложении** представлен листинг исходного кода генератора, описанный пакетом программы VHDL.

ЗАКЛЮЧЕНИЕ

Проведен анализ текущего состояния области генераторов действительно случайных числовых последовательностей. В качестве основы для проектирования ГДСЧП была взята стандартная структура, которая состоит из источника энтропии, схемы сжатия и регистра случайного числа. Реализации каждого из компонентов структуры проанализированы на предмет преимуществ и недостатков, что помогло выбрать в качестве источника энтропии физически неклонируемые функции.

Рассмотрено два типа ФНФ: на основе кольцевых генераторов и на основе статического оперативного запоминающего устройства. В результате рассмотрения классических вариантов реализации источников энтропии было предложено две схемы: модифицированной ФНФ на основе кольцевых генераторов и комбинированной ФНФ. В дополнения к проектам источника энтропии были добавлены схемы сжатия (дерево элементов XOR и LFSR, Адаптивный сигнатурный анализатор соответственно).

Предложено два цифровых устройства, предназначенных для генерирования действительно случайных числовых последовательностей: схема на основе модифицированной ФНФ на базе кольцевых генераторов и схема на основе комбинированной ФНФ.

Разработана методика проведения экспериментов для процесса создания, тестирования и усовершенствования цифровых устройств, направленных на генерирование действительно случайных числовых последовательностей.

Реализованные цифровые устройства были усовершенствованы в результате проведения множества экспериментов, которые позволили:

— подобрать оптимальные значения параметров схем;

— повысить качество генерируемой действительно случайной числовой последовательности;

— уменьшить аппаратные затраты на реализацию цифрового устройства.

Была исследована возможность решения задачи идентификации цифровых устройств с помощью схемной реализации комбинированной ФНФ.

Перспективными направлениями данной работы являются:

— разработка реконфигурируемого ГДСЧП;

— оптимизация временных и аппаратных затрат;

— разработка алгоритмов и методик, направленных на решение задачи идентификации цифровых устройств.

Список опубликованных работ:

[1] Ерминек, К.Р., Вербжицкий, А Использование физически неклонируемых функций для генерирования действительно случайных числовых последовательностей //Информационные технологии, Лодзь – 2014. – №2. с. 63-67.

[2] Ерминек, К.Р., Кочмарска, Защита цифровых устройств при помощи неклонируемых функций //Сборник докладов, Лодзь – 2015. –.с. 15-17

[3] Ерминек, К.Р., Использование физически неклонируемых функций для генерирования действительно случайных числовых последовательностей //Сборник докладов , Плоцк– 2015. –с. 81-83.

.