УДК 681.3.07

СХЕМНАЯ РЕАЛИЗАЦИЯ КОМБИНИРОВАННОЙ ФИЗИЧЕСКИ НЕКЛОНИРУЕМОЙ ФУНКЦИИ ДЛЯ ГЕНЕРИРОВАНИЯ ДЕЙСТВИТЕЛЬНО СЛУЧАЙНЫХ ЧИСЛОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

С.С. ЗАЛИВАКО, А.А. ИВАНЮК

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 28 мая 2013

Исследована возможность применения комбинированной физически неклонируемой функции (на основе статического оперативного запоминающего усройства и на основе кольцевых генераторов) для получения действительно случайных числовых последовательностей. Сгенерированные последовательности успешно проходят статистические тесты NIST и Diehard. Исследована возможность решения задачи идентификации цифровых устройств с использованием физически неклонируемой функции на основе статического оперативного запоминающего устройства. Полученные в результате эксперимента метрики расстояний говорят о возможности использования такой методики для решения задачи идентификации.

Ключевые слова: физически неклонируемые функции, статическое оперативное запоминающее устройство, кольцевой генератор, идентификация цифрового устройства, генератор действительно случайных чисел, адаптивный сигнатурный анализ.

Введение

Многие производители интегральных схем решают задачу идентификации цифрового устройства путем реализации специальных регистров хранения уникальных идентификаторов (серийных номеров), значения которых, как правило, единожды задаются на этапе производства и в последующем использовании доступны только для чтения.

Данный подход имеет значительный недостаток: большинство серийно выпускаемых ПЛИС не содержит регистров для хранения уникальных идентификаторов, поэтому пользовательская реализация таких регистров не защищена от клонирования злоумышленником. В связи с этим необходима процедура создания и проверки такого идентификатора, который бы соответствовал требованиям уникальности, неклонируемости, непредсказуемости. Использование физически неклонируемых функций для создания идентификатора позволяет удовлетворить требованиям, описанным выше.

Как показали исследования других авторов [1], класс используемых в данной работе физически неклонируемых функций может быть использован в качестве источника для генерирования действительно случайных числовых последовательностей.

Таким образом, основными задачами данной работы являются: исследование физически неклонируемых функций на возможность генерирования действительно случайной числовой последовательности (ГДСЧП), а также на возможность генерирования уникального идентификатора цифрового устройства.

Физически неклонируемые функции

Физически неклонируемая функция (англ. Physical Unclonable Function (PUF)) – это функция, воплощенная в физической структуре, которую просто оценить, но трудно

охарактеризовать, смоделировать или воспроизвести. Изначально идея использования ФНФ принадлежит Р. Паппу [2, 3]. Одно из наиболее широко используемых на сегодняшний день определений ФНФ было предложено П. Туилсом [4]. ФНФ, по Туилсу, – это физические системы (устройства), неотъемлемым свойством которых является неклонируемость (неповторяемость) некоторых их функций, свойств, характеристик либо параметров.

ФНФ описываются значениями пар входных и соответствующих им выходных параметров (сигналов). Подобная пара, состоящая из входного физического параметра (запроса) и выходного параметра (ответа), называется парой запрос–ответ (Challenge-Response Pair, CRP). В простейшем случае ФНФ можно рассматривать как функцию, которая преобразует запросы C_i в ответы R_i [4]:

$$R_i = PUF\ (C_i). \qquad (1)$$

ФНФ обладает двумя важными свойствами: практически невозможно создать физическую копию ФНФ; невозможно создать точную математическую модель ФНФ, то есть вычислить отклик, если даны точные параметры запроса и другие пары запросов-откликов. Из-за сложности физического взаимодействия эта задача представляет большие вычислительные трудности.

Эти качества вместе и называются неклонируемостью.

Схемная реализация комбинированной физически неклонирумой функции

За основу схемной реализации была взята ФНФ на основе статического ОЗУ [5]. Аппаратно данный тип ФНФ может быть реализован на основе двух инверторов и мультиплексора. Схема приведена на рис. 1.

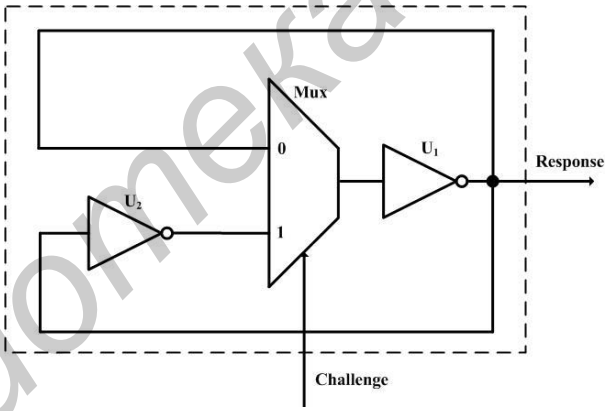


Рис. 1. Схема комбинированной ФНФ

Данная схема в зависимости от управляющего сигнала *Challenge* может работать в двух режимах: RO-PUF (Ring Oscillator PUF), SRAM PUF (Static Random Access Memory PUF) [5].

В режим RO-PUF схема переходит, когда значение управляющего сигнала *Challenge* = 0. В этом режиме цифровое устройство работает как ФНФ типа кольцевой генератор. Свойства данного типа ФНФ более подробно описаны авторами в работе [6]. Заметим, что описываемый режим может быть использован в качестве источника энтропии для генерирования действительно случайной числовой последовательности.

В случае, когда значение *Challenge* = 1, схема работает в режиме SRAM PUF. При каждом включении цифрового устройства в данном режиме ФНФ эмулирует поведение ячейки памяти, которая «хранит» бит информации. При этом ячейка памяти может постоянно принимать значение логического нуля (единицы) или же изменять свое значение от запуска к запуску. Описанные выше свойства SRAM PUF и будут использованы для получения уникального идентификатора цифрового устройства.

Структура цифрового устройства, которое может быть построено на базе ячеек, функционирование которых описано выше, приведена на рис. 2.

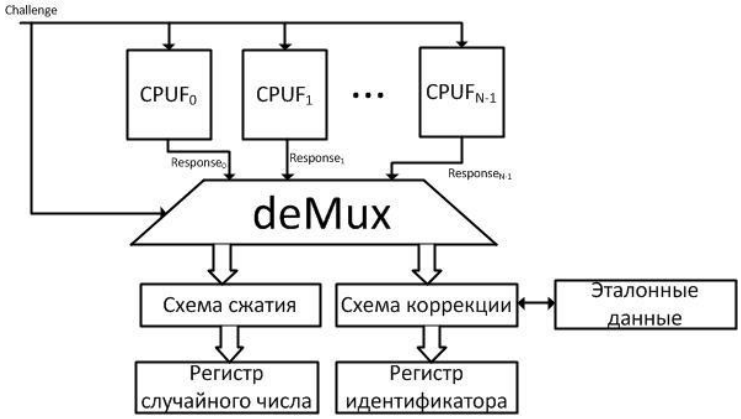


Рис. 2. Структура предлагаемого устройства

В общем случае устройство состоит из трех структурных блоков: совокупности ячеек ФНФ, схемы сжатия (для ГДСЧП) или схемы коррекции (для идентификации) и регистра, который хранит либо случайное число, либо идентификатор цифрового устройства.

В качестве схемы сжатия могут быть использованы различные схемные решения: дерево элементов XOR [7], линейный сдвиговый регистр с обратной связью (Linear feedback shift register – LFSR) [8], корректор Фон-Неймана [9], адаптивный сигнатурный анализатор [10].

Методика проведения эксперимента

Эксперимент проводился на двух идентичных ПЛИС Xilinx Spartan 3E-500 FG320, входивших в состав двух плат B_0 и B_1. Для двух плат было сгенерировано по 100 64-битных идентификатора.

Эксперимент состоял из четырех этапов:

1) составление vhdl-проекта;
2) 100 раз совершались следующие действия:
   2.1) программирование ПЛИС;
   2.2) получение значения идентификатора через интерфейс USB;
   2.3) переход к пункту 2.1;
3) анализ данных, полученных в результате эксперимента;
4) корректировка vhdl-описания.

Для получения последовательности действительно случайных чисел применялся адаптивный сигнатурный анализ на этапе 3 [10]. Каждый из полученных на этапе 2 идентификаторов с использованием соотношения (2) преобразуется в случайное число из диапазона [0;63].

$$S = \oplus_{i=0}^{2^N-1} A_i, \forall R[A_i] = 1, \quad (2)$$

где A_i – адрес ячейки памяти (число в диапазоне $[0;2^N-1]$), N – количество ячеек SRAM PUF, R – N-битное число, которое является идентификатором, $R[i]$ – бит, который хранится в ячейке с адресом i.

Анализ данных производился с помощью пакета прикладных программ Statistica, пакетов статистических тестов NIST [11] и Diehard.

Генерирование последовательности случайных чисел с помощью RO-PUF

В случае, когда управляющий сигнал *Challenge* = 0, каждая из ячеек, описанных выше, работает как ФНФ типа кольцевой генератор. Выход каждой из ячеек подается на вход адаптивного сигнатурного анализатора, результатом работы которого предположительно будет элемент действительно случайной числовой последовательности.

Сгенерированные последовательности размером $6 \cdot 10^7$ бит были протестированы с помощью пакета NIST. Каждая из последовательностей поделена пакетом на 1000 выборок по 60000 бит. Результаты тестирования приведены в табл. 1.

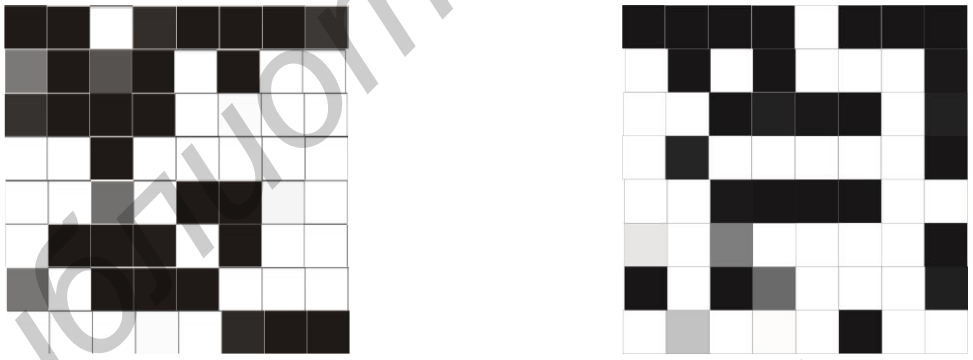
Таблица 1**. Результаты статистического тестирования последовательности с помощью пакета NIST**

Название статистического теста	Процент выборок, прошедших тест
Частотный тест	100,0
Частотный блочный тест	100,0
Тест на последовательность одинаковых бит	100,0
Тест на самую длинную последовательность единиц в блоке	100,0
Тест рангов бинарных матриц	100,0
Спектральный тест	100,0
Тест неперекрывающихся шаблонов	148/148 (среднее 95,0)
Тест перекрывающихся шаблонов	90,0
Универсальный статистический тест Маурера	100,0
Тест на линейную сложность	90,0
Тест на периодичность	100,0 / 100,0
Тест приблизительной энтропии	100,0
Тест куммулятивных сумм	100,0/100,0
Тест на произвольные отклонения	8/8 (среднее 92,9)
Другой тест на произвольные отклонения	16/16 (среднее 93,5)

Как видно из таблицы, все статистические тесты NIST успешно пройдены, что свидетельствует о том, что адаптивный сигнатурный анализатор может быть использован в качестве схемы сжатия даже более успешно, чем исследованные авторами дерево элементов XOR совместно с LFSR [6].

Генерирование последовательности случайных чисел с помощью SRAM PUF

При значении управляющего сигнала *Challenge* = 1 каждая из ячеек работает как ФНФ на основе статического ОЗУ. В результате эксперимента были получены карты памяти «SRAM PUF» для плат B_0 и B_1, которые, в свою очередь, могут являться уникальными идентификаторами плат.



а *б*

Рис. 3. Карты памяти «SRAM PUF»: *а* – для платы B_0; *б* – для платы B_1

На рис. 3 приведено графическое изображение карт памяти для каждой из плат. Черным цветом обозначается ячейка SRAM PUF, которая хранит логическую единицу, белым – логический ноль. Оттенки серого обозначают вероятность хранения в данном регистре единицы. Например, если вероятность хранения в регистре единицы составляет 0,3, то он будет изображен серым цветом, в котором доля черного составляет 30 %, а доля белого – 70 %. Как видно из рисунка карты памяти отличаются значительно уже на 64 ячейках SRAM PUF.

Данные графического теста подтверждаются различными метриками расстояний между идентификаторами: Евклидово расстояние, расстояние городских кварталов (Манхэттенское), расстояние Минковского, косинусное расстояние, корреляционное расстояние, расстояние Хэмминга, расстояние Джаккарда [12].

«Эталонной» картой назовем такой *N*-битный идентификатор, каждый бит которого принимает значение из следующего соотношения:

$$\begin{cases} 0, p_i^* < 0{,}5 \\ 1, p_i^* \geq 0{,}5 \end{cases}, \quad (3)$$

где p_i^* – наблюдаемая вероятность появления единицы.

Например, для карты, приведенной на рис. 3а «эталонная» карта будет выглядеть так «1101111111110100111100000010000000001100011101000011100000000111».

В табл. 2 приведены средние, максимальные и минимальные значения метрик, описанных выше.

Таблица 2**. Метрики расстояний между идентификаторами прототипных плат**

Метрика расстояния	Минимальное расстояние	Максимальное расстояние	Среднее расстояние	Расстояние между «эталонными» картами
Евклидово расстояние	4,58257	5,29150	4,90749	5,19615
Расстояние городских кварталов	21,0000	28,0000	24,11000	27,00000
Расстояние Минковского (p = 3)	7,00000	9,33333	8.03667	9,00000
Расстояние Хэмминга	0,32812	0,43750	0,37672	0,421875
Корреляционное расстояние	0,66386	0,89579	0,76400	0,85820
Косинусное расстояние	0,27994	0,39975	0,33585	0,49015
Расстояние Джаккарда	0,32812	0,43750	0,37672	0,42188

Данные, приведенные в табл. 2, свидетельствуют о том, что два идентифицируемых объекта (ПЛИС) отличаются значительно. Этот факт позволяет выдвинуть гипотезу о том, что идентификатор, построенный по принципам, описанным выше, позволит однозначно распознавать цифровое устройство.

Экспериментально установлено, что на одной и той же плате появление одной же карты памяти маловероятно (наблюдаемая вероятность для 64-битной карты составляет 0,02). Большая часть битов является стабильной (81,25 %), поэтому «карту памяти» SRAM можно использовать в качестве основы для построения идентификатора.

Был также проведен эксперимент по генерированию идентификаторов на одной и той же плате, но с изменением топологии блоков комбинационной логики. Средние значения расстояние городских кварталов для трех различных топологий приведены в табл. 3.

Таблица 3**. Метрики расстояний между идентификаторами, сгенерированными на одной плате, но с помощью разных топологий**

Тип топологии	Топология T_0	Топология T_1	Топология T_2
Топология T_0	0,0	27,05	33,26
Топология T_1	27,05	0,0	29,25
Топология T_2	33,26	29,25	0,0

Таким образом, физически неклонируемая функция на основе статического ОЗУ может быть источником уникального идентификатора, поскольку ее поведение определяется не только ПЛИС, но и проектом, загружаемым в ПЛИС.

На основе идентификаторов, генерируемых при каждом запуске устройства, может быть построена последовательность действительно случайных чисел. Такая последовательность получается в результате сжатия исходной последовательности адаптивным сигнатурным анализатором. На данной 64-битной карте возможно получать действительно случайные числа в диапазоне [0;63].

Был проведен эксперимент по генерированию последовательности действительно случайных чисел в диапазоне [0;511] объемом $6 \cdot 10^7$ бит. Гистограмма плотности распределения последовательности действительно случайных чисел, полученной предлагаемым цифровым устройством показана на рисунке.

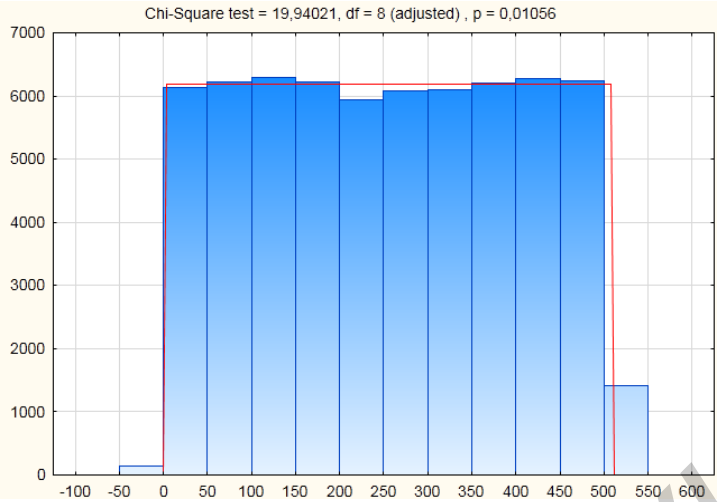


Рис. 4. Гистограмма плотности распределения действительно случайной числовой последовательности

Тестирование генератора производилось с помощью двух статистических пакетов NIST и Diehard.

Пакет статистических тестов NIST состоит из 15 тестов. Результаты тестирования последовательности (она была поделена пакетом на 1000 выборок по 60000 бит) приведены в таблице.

Таблица 4**. Результаты статистического тестирования последовательности с помощью пакета NIST**

Название статистического теста	Процент выборок, прошедших тест
Частотный тест	100,0
Частотный блочный тест	100,0
Тест на последовательность одинаковых бит	100,0
Тест на самую длинную последовательность единиц в блоке	100,0
Тест рангов бинарных матриц	100,0
Спектральный тест	100,0
Тест неперекрывающихся шаблонов	148/148 (среднее 95,0)
Тест перекрывающихся шаблонов	100,0
Универсальный статистический тест Маурера	100,0
Тест на линейную сложность	100,0
Тест на периодичность	100,0 / 100,0
Тест приблизительной энтропии	100,0
Тест куммулятивных сумм	100,0/100,0
Тест на произвольные отклонения	8/8 (среднее 100,0)
Другой тест на произвольные отклонения	16/16 (среднее 100,0)

Как видно из таблицы, все тесты успешно проходят на более чем 95 % выборок, и так как пакет тестируемых данных достаточно велик, то можно говорить о том, генерируемые последовательности обладают хорошими статистическими свойствами и практически не уступают по качеству эталонным статистическим последовательностям.

Заключение

Разработана схемная реализация комбинированной физически неклонируемой функции (на основе статического ОЗУ и на основе кольцевых генераторов). Предлагаемая реализация может быть использована в качестве базы для цифрового устройства, которое может быть использовано как генератор действительно случайных числовых последовательностей.

Источником случайности в ГДСЧП выступает либо ФНФ на основе кольцевых генераторов либо на основе статического ОЗУ, в качестве схемы сжатия предлагается адаптивный сигнатурный анализатор.

Получаемая с помощью описанного устройства действительно случайная числовая последовательность имеет хорошие статистические свойства, что подтверждается прохождением генерируемыми последовательностями всех тестов из пакетов NIST и Diehard.

Разработанное цифровое устройство также может быть использовано для решения задачи идентификации. Эксперимент на небольшой разрядности идентификатора показал, что данный способ его получения является перспективным и может использоваться в различных системах безопасности, а также для защиты от копирования, клонирования, подделки различных цифровых устройств.

Одним из перспективных направлений развития данной работы является разработка схемы корректировки идентификатора с целью стабилизации его значения.

COMBINED PHYSICAL UNCLONABLE FUNCTION CIRCUIT IMPLEMENTATION FOR GENERATION TRUE RANDOM NUMBER SEQUENCES

S.S. ZALIVAKO, A.A. IVANIUK

Abstract

The possibility of using two physical unclonable functions (based on static random access memory and on the ring oscillators) to produce true random number sequences was investigated. Generated sequences successfully pass NIST and Diehard statistical tests. The possibility of solving the digital devices identification problem using physical unclonable function based on static RAM was investigated. Experimentation data (distances metric between digital devices identifiers) showed the possibility of using such technique for solving the problem of identification.

Список литературы

1. *Holcomb D.E.* // IEEE Trans. Computers. 2009. Vol. 58. P. 1198–1210.
2. *Pappu R.* Physical One-Way Functions // Science. 2002. Vol. 297. P. 2026–2030.
3. *Pappu R.* Physical One-Way Functions: PhD Thesis in Media Arts and Sciences. Cambridge, 2001.
4. *Tuyls P.* Security with Noisy Data. London, 2007.
5. *Иванюк А.А.* Проектирование встраиваемых цифровых устройств и систем: монография. Минск, 2012.
6. *Заливако С.С., Иванюк А.А.* // Матер. Междунар. научн. Конф. «ИТС 2012». Минск, 24 октября 2012. С. 202–203.
7. *Maiti A., Nagesh R., Reddy A. et. al.* // 19th Great Lakes Symposium on VLSI. May, 2009.
8. *Ярмолик В.Н., Демиденко С.Н.* Генерирование и применение псевдослучайных сигналов в системах испытания и контроля. Минск, 1986.
9. *Danger J.-L., Guilley S., Hoogvorst P.* // Microelectronics journal. 2009. № 40. P. 1650–1656.
10. *Иванюк А.А., Ярмолик В.Н.* Проектирование контролепригодных цифровых устройств. Минск, 2006.
11. *Rukhin A.A* Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Application. NIST special publication, 2010.
12. *Айвазян С.А., Бухштабер И.С., Енюков В.М. и др.* Прикладная статистика: Классификация и снижение размерности. М.,1989.