УДК 004.056.53

ИСПОЛЬЗОВАНИЕ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ ДЛЯ РЕШЕНИЯ ЗАДАЧИ ГЕНЕРИРОВАНИЯ ДЕЙСТВИТЕЛЬНО СЛУЧАЙНЫХ ЧИСЕЛ И ИДЕНТИФИКАЦИИ

С.С. ЗАЛИВАКО[1], А.А. ИВАНЮК[2]

[1]Nanyang Technological University
50 Nanyang Avenue, Singapore 639798
zali0001@e.ntu.edu.sg

[2]Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
ivaniuk@bsuir.by

Исследована возможность применения физически неклонируемой функции на основе статического ОЗУ для решения задачи генерирования последовательности действительно случайных чисел, а также идентификации цифровых устройств. Разработанная схемная реализация в силу своей универсальности может одновременно решать две задачи, используя два различных механизма обработки генерируемых значений.

Ключевые слова: физически неклонируемая функция на основе статического ОЗУ, генерирование действительно случайных числовых последовательностей, идентификация цифровых устройств.

В настоящее время цифровые устройства (ЦУ) и их проектные описания нередко подвергаются нелегальному копированию, клонированию и перепроизводству. Одним из способов защиты прав производителей является уникальная идентификация ЦУ и их проектных описаний. Данную задачу производители решают различными способами: физическое нанесение серийных номеров; сохранение идентификатора в регистрах, предназначенных только для чтения; идентификация на уровне функционирования; активное измерение и др. В данной работе предлагается для решения этой задачи использовать физически неклонируемые функции (ФНФ) [1]. ФНФ, по Туилсу [1], – это физические системы (устройства), неотъемлемым свойством которых является неклонируемость (неповторяемость) некоторых их функ-ций, свойств, характеристик либо параметров.

Для решения задачи идентификации цифровых устройств предложена комбинированная ФНФ [2], которая в зависимости от управляющего сигнала *Challenge* может работать в двух режимах: RO-PUF (Ring Oscillator PUF), SRAM PUF (Static Random Access Memory PUF) [3]. В данной работе мы рассмотрим режим SRAM PUF. В этом режиме значение сигнала *Challenge* = 1, что позволяет эмулировать поведения ячейки памяти, «храня-щей» один бит информации. При этом ячейка памяти может постоянно принимать зна-чение логического нуля (единицы) или же изменять свое значение от запуска к запуску. Описанные выше свойства SRAM PUF и будут использованы для получения уникаль-ного идентификатора цифрового устройства.

Предлагаемое устройство, построенное на основе ФНФ имеет структуру, представленную на рис. 1. В общем случае устройство состоит из трех структурных блоков: N ячеек ФНФ, схемы сжатия (для генерирования последовательности действительно случайных чисел) или схемы коррекции (для идентификации) и регистра, который хранит либо случайное число, либо идентификатор цифрового устройства.

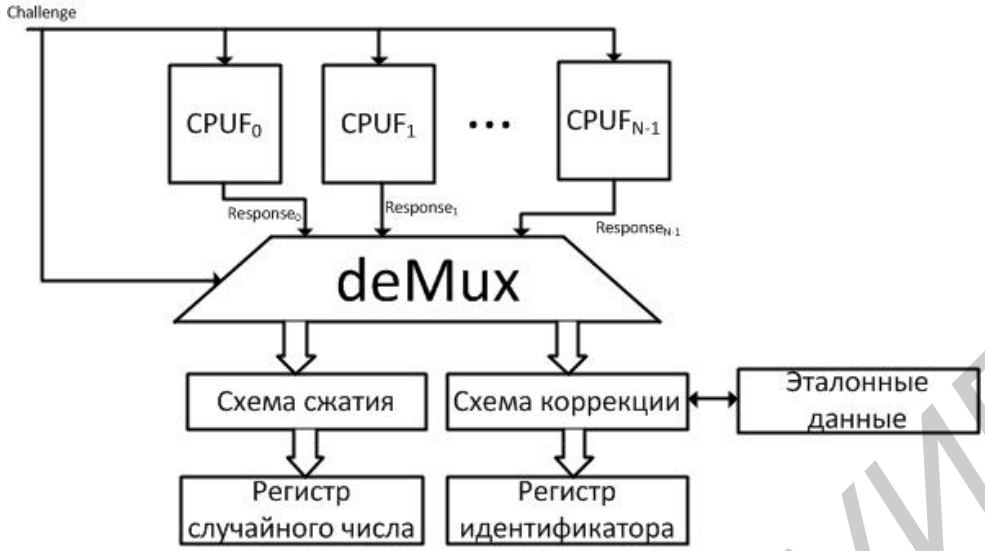

Рис. 1. Структура предлагаемого устройства

В качестве схемы сжатия был использован адаптивный сигнатурный анализатор [4], а для схемы коррекции предлагается использовать коды коррекции ошибок (например, код Хэмминга). Для проверки гипотезы исследования был проведен эксперимент (на двух иден-тичных ПЛИС Xilinx Spartan 3E-500 FG320, входивших в состав двух плат B_0 и B_1), который состоял в том, что данное устройство включалось и выключалось 10^6 раз и каждый раз на вход подавалось 64-битное значение запроса. В результате чего получался 64-битный отклик, который и являлся уникальным идентификатором цифрового устройства. Поскольку работа ФНФ является нестабильной, то идентификатор для каждого устройства получался по правилу максимального правдоподобия (если в результате n (не менее 100) экспериментов вероятность появления единицы больше чем нуля в определенной ячейке, то за бит идентификатора берется значения единицы, иначе – нуля). Эксперименты показали, что для 64-битных идентификаторов расстояние Хэмминга между устройствами составляет порядка 24.

На основе нестабильности идентификаторов также был построен генератор действительно случайных числовых последовательностей (ГДСЧП). На основе множества идентификаторов с применением адаптивного сигнатурного анализатора были сгенерированы последовательности 8-битных чисел, объемом $6 \cdot 10^7$ бит. Тестирование этих последовательностей пакетами NIST и Diehard показало, что они соответствуют критериям действительной случайности. Также на уровне значимости $\alpha = 0{,}05$ было подтверждено, что последовательности, сгенерированные на различных платах B^0 и B^1, не обладают корреляционной зависимостью. Таким образом, две абсолютно противоположные задачи (идентификации и ГДСЧП) могут быть успешно решены с помощью одной и той же схемы комбиниро-ванной ФНФ. Метрики расстояний показывают хорошую степень идентификации, а прохождение тестов NIST и Diehard – качество последовательности случайных чисел.

Список литературы

1. *Toils, P.* Security with Noisy Data. London, 2007.
2. *Заливако, С.С., Иванюк, А.А.* // Доклады БГУИР. 2013. № 7 (77). С. 37-43.
3. *Иванюк, А.А.* Проектирование встраиваемых цифровых устройств и систем: монография. Минск, 2012.
4. *Иванюк, А.А., Ярмолик, В.Н.* Проектирование контролепригодных цифровых устройств. Минск, 2006.