УДК 004.3, 681.5

АНАЛИЗ ХАРАКТЕРИСТИК ФИЗИЧЕСКИ НЕКЛОНИРУЕМОЙ ФУНКЦИИ ТИПА АРБИТР НА FPGA ARTIX-7

Шамына А.Ю., аспирант

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Иванюк А.А. – д-р техн. наук, профессор

В данной работе произведен анализ характеристик случайности, уникальности и стабильности физически неклонируемых функций типа арбитр (А-ФНФ) различных реализаций. Кратко описано построение экспериментальной установки для исследования. Показана зависимость характеристик от длин блока симметричных путей А-ФНФ.

Ключевые слова: физически неклонируемые функции, АФНФ, ПЛИС, FPGA, Artix-7, платы быстрого прототипирования.

Физически неклонируемые функции (ФНФ) широко применяются в различных сферах: генераторы истинно случайных числовых последовательностей, протоколы аутентификации и проверки подлинности, криптографические примитивы и т.д. Ввиду относительно низких аппаратурных затрат и простоты реализации довольно популярны ФНФ типа арбитр (А-ФНФ) [1]. Принцип работы А-ФНФ основывается на извлечении уникальной для каждой реализации трансляции тестовых сигналов через каскад последовательно соединенных мультиплексоров, конфигурация которых определяется значением запроса. В А-ФНФ выделяют следующие структурные компоненты: генератор тестовых сигналов (ГТС), блок симметричных путей (БСП), а также арбитр, отвечающий за выработку ответа ФНФ (рисунок 1).

Основными характеристиками любой ФНФ являются случайность, уникальность и стабильность. Для исследования указанных характеристик были реализованы А-ФНФ с различными длинами БСП (от 8 до 256 блоков), а также с несколькими вариантами схем арбитров (RS-защелка и D-триггер). Проектное описание экспериментальной установки было создано с использованием САПР Vivado 2018.2 на языке VHDL. Кроме реализации А-ФНФ, экспериментальная установка включает в себя описание генератора М-последовательности на основе linear feedback shift register (LFSR), а также устройства управления в виде цифрового конечного автомата (ЦКА).

Для организации передачи экспериментальных данных между установкой и ПК через интерфейс UART был использован софт-процессор Mircroblaze.

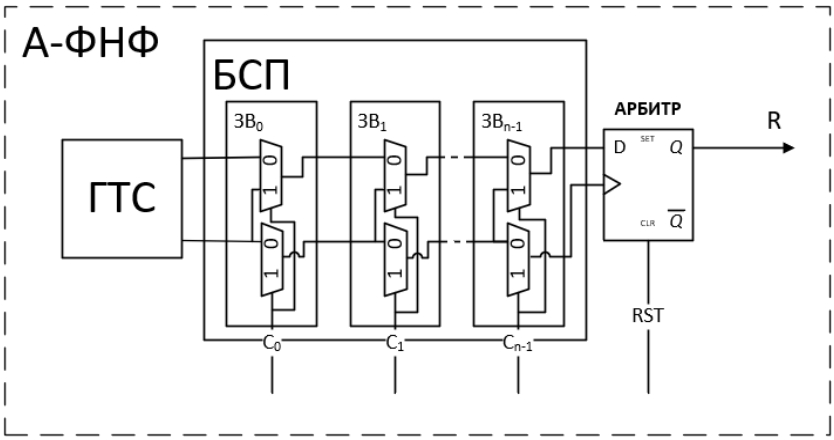

Рисунок 1 – Структура А-ФНФ

Использование софт-процессора, а также IP-компонентов позволило существенно сократить время на разработку. В качестве аппаратной базы были выбраны платы быстрого прототипирования Nexys 4 фирмы Digilent с FPGA Artix-7. Общая схема эксперимента представлена на рисунке 2.

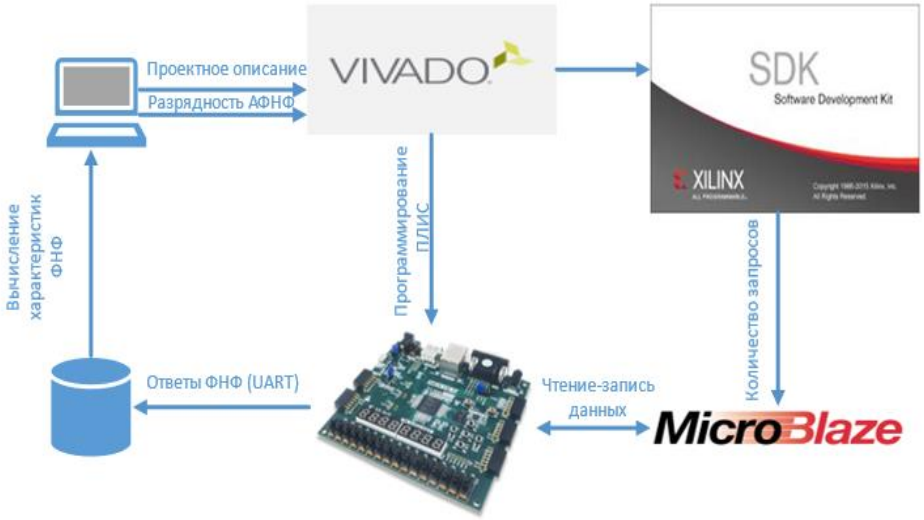

Рисунок 2 – Общая схема эксперимента

Для анализа характеристик А-ФНФ для каждой реализации было проведено E=10 экспериментов на M=2 кристаллах. Каждый эксперимент предполагал генерацию 10^6 запросов к ФНФ и получение такого же количества ответов. После сбора данных были высчитаны характеристики стабильности, случайности и уникальности А-ФНФ. Следует также отметить, что для анализа зависимости характеристик А-ФНФ с различными длинами БСП арбитры были подключены не только к последнему звену А-ФНФ, как это предполагает классическая реализация А-ФНФ, но и к промежуточным узлам БСП, что позволило за один эксперимент собрать данные для А-ФНФ с различным количеством звеньев в БСП.

Для расчета характеристики стабильности $S(CH)$ ответа ФНФ R на запрос CH использовалась следующая формула (1):

$$S(CH) = 1 - \frac{1}{E}\sum_{e=1}^{E} HD\left(R_{ref}, R_e\right), \quad (1)$$

где E – количество экспериментов;
e – индекс эксперимента;
HD – расстояние Хемминга;
R_{ref} – эталонное значение ответа на заданный запрос, определяемое по мажоритарному принципу;
R_e – ответ на заданный запрос.

Оценка стабильности каждой реализации А-ФНФ производилась по среднему значению, вычисляемому как среднее арифметическое всех значений стабильности каждого выполненного запроса к конкретной реализации А-ФНФ, и определяется формулой (2):

$$S_{avg} = \frac{1}{K}\sum_{i=1}^{K} S(CH_i), \quad (2)$$

где *K* – количество запросов;
i – индекс запроса.

Показатель минимальной стабильности определяется выражением (3):

$$S_{min} = \min(S(CH_1), S(CH_2), \dots, S(CH_k)). \quad (3)$$

Для всех А-ФНФ, реализованных в данном эксперименте, минимальное значение стабильности S_{min} составило 0,5. Такой результат объясняется эффектом метастабильности арбитра А-ФНФ при генерации ответа на определенные запросы. Минимизировать негативный эффект метастабильности арбитра позволяет применение подходов на основе кодов коррекции либо изменение схемы арбитра.

В качестве характеристики случайности была принята доля ответов А-ФНФ *R* =1. За показатель стабильности была принята доля запросов к А-ФНФ, соответствующие ответы на которые были неизменны для каждого повтора эксперимента. Гистограммы характеристик А-ФНФ, полученные в результате проведенных экспериментов, представлены на рисунках 3 и 4.

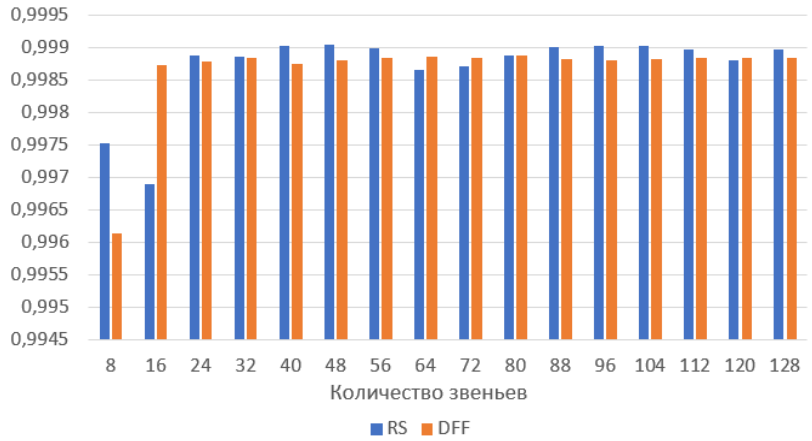

Рисунок 3 – Гистограмма значений полученной характеристики стабильности А-ФНФ

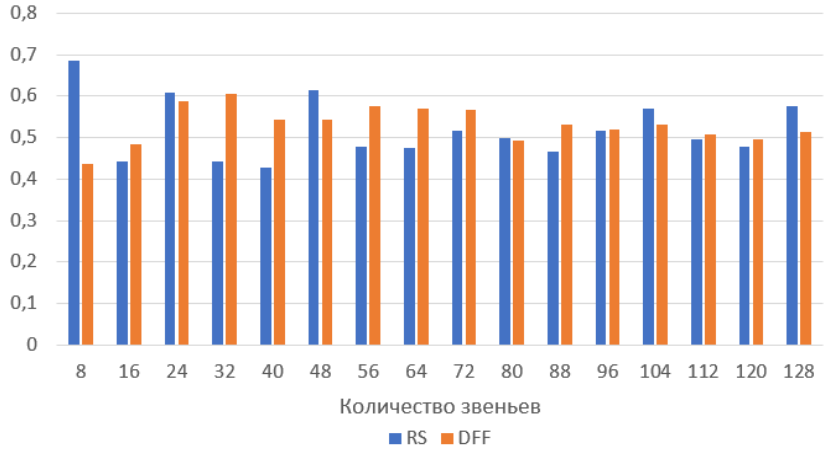

Рисунок 4 – Гистограмма значений полученной характеристики случайности А-ФНФ

Однако полученные средние значения межкристальной уникальности оказались низкими (2 и 7 процентов для А-ФНФ с RS-защелкой и D-триггера соответственно). Множественные попытки изменения стратегии синтеза и имплементации А-ФНФ на FPGA при неизменных длинах БСП и видах арбитров не оказали существенного влияния на данную характеристику. Только увеличение длины БСП до 256 звеньев позволило достичь уникальности 49 %. Показатель уникальности вычислялся как доля различных ответов на одни и те же запросы для полностью стабильных ответов, полученных в результате эксперимента.

Исходя из полученных результатов, можно сделать вывод об улучшении характеристик А-ФНФ при увеличении длины БСП. Однако при этом возрастают аппаратные затраты и увеличивается время получения ответа А-ФНФ. Поиск решений для улучшения заданных характеристик будет предметом дальнейших исследований.

Список использованных источников:

1. Заливако, С. С. Физически неклонируемые функции / С. С. Заливако, А. А. Иванюк // Информационные технологии и системы 2019 (ИТС 2019) = Information Technologies and Systems 2019 (ITS 2019) : материалы международной научной конференции, Минск, 30 октября 2019 г. / Белорусский государственный университет информатики и радиоэлектроники ; редкол. : Л. Ю. Шилин [и др.]. – Минск, 2019. – С. 8–21.

2. Nexys 4 artix-7 FPGA: Trainer board recommended for ece curriculum [Electronic resource]. Mode of access : https://store.digilentinc.com/nexys-4-artix-7-fpga-trainer-board-limited-time-see-nexys4-ddr/. Digilent, Inc, 2021. Date of access : 04.04.2021.

UDC 004.3, 681.5

ANALYSIS OF THE CHARACTERISTICS OF ARBITER PUF ON FPGA ARTIX-7

Shamyna A.Y.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Ivaniuk A.A. – D. Sc. (Technology)

In present work the characteristics of randomness, uniqueness and stability of physical unclonable functions of the arbiter type (A-PUF) of various implementations are considered. The construction of an experimental setup for research is briefly described. The dependence of the characteristics on the block lengths of symmetric A-PUF paths is shown.

Keywords: physical unclonable functions, A-PUF, FPGA, Artix-7, Nexys 4.