КОНФИГУРАЦИЯ СИММЕТРИЧНЫХ ПУТЕЙ ФИЗИЧЕСКИ НЕКЛОНИРУЕМОЙ ФУНКЦИИ ТИПА АРБИТР НА FPGA

Шамына А.Ю., аспирант

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

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

Аннотация. В работе рассматривается синтез симметричных путей физически неклонируемой функции типа арбитр, построенной на базе звеньев, каждое из которых функционально представляет собой два повторителя, которые реализованы на основе компонентов LUT6 одного slice-блока FPGA. Описывается способ устранения асимметрии межсоединений на основе управляемых линий задержки. Рассчитаны временные характеристики симметричных путей предложенной структуры для нескольких конфигураций.

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

В настоящее время все большая роль и значение отводятся средствам физической криптографии. Одним из наиболее популярных направлений является изучение физически неклонируемых функций (ФНФ) [1]. Основополагающая идея ФНФ заключается в извлечении характеристик, свойственных конкретной физической системе, которые являются уникальными и неповторяемыми, но при этом достаточно стабильными и удовлетворяющими определённым критериями при их многократном извлечении. Большинство ФНФ, реализованных в составе цифровых устройств, основаны на вариативности задержек распространения сигналов по фиксированным путям идентичных с точки зрения проектного описания и технологии изготовления интегральных схем. Это свойство обусловлено естественными флуктуациями в материалах, используемых при производстве данных устройств, а также некоторым несовершенством производственного процесса.

Популярным схемотехническим решением, позволяющим на основе уникальности задержек распространения сигналов по топологически одинаковым путям различных экземпляров одного устройства генерировать уникальную битовую последовательность для некоторого множества фиксированных запросов, является использование так называемых физически неклонируемых функций типа арбитр (АФНФ) [2, 3].

Классическая схема АФНФ подразумевает наличие генератора тестового сигнала, блока симметричных путей (БСП) и арбитра, который позволяет определить очередность прохождения фронтов тестового импульса через блок симметричных путей и выработать на этой базе ответ R. В свою очередь, блок симметричных путей представляет собой последовательно соединенные звенья, которые, как правило, строятся с использованием двух мультиплексоров с конфигурацией 2x1 и обеспечивают прямую, либо перекрестную передачу двух тестовых сигналов в зависимости от значения разряда запроса.

Однако при реализации АФНФ на современных FPGA, таких как Artix 7 фирмы Xilinx, возникает ситуация неполного использования ресурсов LUT-компонентов. Так, для реализации звена пути классической АФНФ требуется два LUT3, хотя фактически используются два LUT6 и значительная часть их ресурсов остается незадействованными. Потенциально более полное использование ресурсов предоставляемых технологических компонентов FPGA может значительно сократить совокупные аппаратные затраты при реализации АФНФ и улучшить их характеристики.

В настоящей работе предлагается в качестве звена БСП использовать схему двух функциональных повторителей, которые будут полностью использовать ресурсы LUT6 и обеспечивать 32 уникальные трансляции в зависимости от 5-разрядного запроса. Уникальность задержки сигнала при этом объясняется отличием пути прохождения сигнала непосредственно внутри самого LUT-блока в зависимости от значений сигналов на его адресных входах. Таким образом, например, при реализации 128-разрядной АФНФ предложенная архитектура БСП позволяет сократить использование технологических LUT-компонентов в пять раз при неизменной мощности множества запросов и ответов. Технологический синтез полученного звена представлен на рисунке 1.

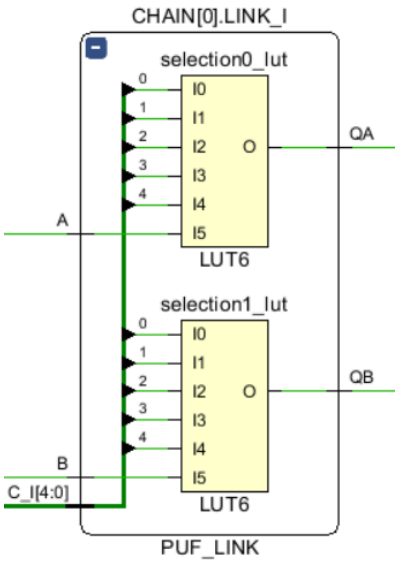

Рисунок 1 – Технологический синтез предложенной схемы звена БСП

Для измерения временных характеристик задержек в работе была использована схема кольцевого осциллятора (КО), где входы и выходы БСП были охвачены петлей обратной связи. Также в данную цепь обратной связи был добавлен элемент NAND для обеспечения управления полученной схемой измерения. Измерение частоты генерируемой импульсной последовательности КО осуществлялось с использованием синхронного счетчика, который для каждого измерения работал одинаковое время.

Проектное описание экспериментальной установки, в которой кроме самостоятельно описанных модулей широко использовались IP-ядра и софт-процессор Microblaze, было создано в САПР Vivado 2018.2 с использованием языка VHDL. Эксперимент проводился на пяти идентичных платах быстрого прототипирования Digilent Nexys 4 с FPGA Artix 7. Каждый эксперимент включал генерацию C=10^5 запросов и повторялся M=10 раз.

Результаты эксперимента для N=128 представлены в виде графика на рисунке 2.

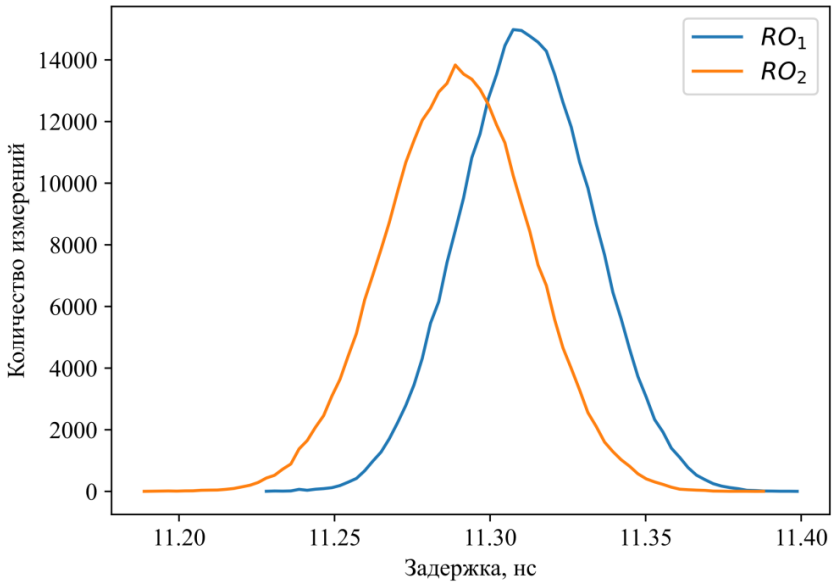

Рисунок 2 – Временное распределение задержек для конфигурации N=128

Из рисунка 2 видно, что для двух полученных путей выбранной конфигураций БСП характерен взаимный временной сдвиг полученных значений измерений задержек, что может негативно сказаться на характеристиках АФНФ. Данное явление обусловлено асимметрией межсоединений slice-блоков FPGA, которые при автоматизированном синтезе носят неуправляемый характер. Для нивелирования данного эффекта была использована линия управляемой задержки, которая представляет собой последовательно соединенные повторители. Также линия задержки включает в себя мультиплексор, который на основе запроса включает в

линию задержки определенное количество элементов, тем самым изменяя совокупное значение задержки. В данной работе 2 управляемые линии задержки были подключены к выходам БСП для возможности корректировки их асимметрии. Затем для текущей конфигурации была подобрана комбинация селектирующих сигналов на линиях управляемых задержек, обеспечивающая минимальную асимметрию задержек для двух исследуемых путей АФНФ. Затем данная комбинация селектирующих сигналов фиксировалась на линиях задержки при проведении эксперимента. Полученные результаты для *N*=128 и *N*=256 представлены на рисунках 3 и 4 соответственно.

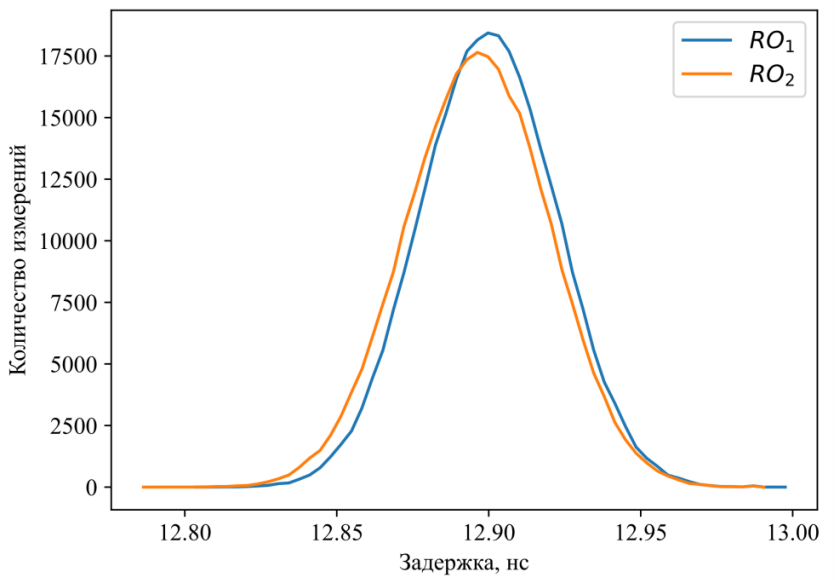

Рисунок 3 – Временное распределение задержек для конфигурации *N*=128 с управляемой линией задержки

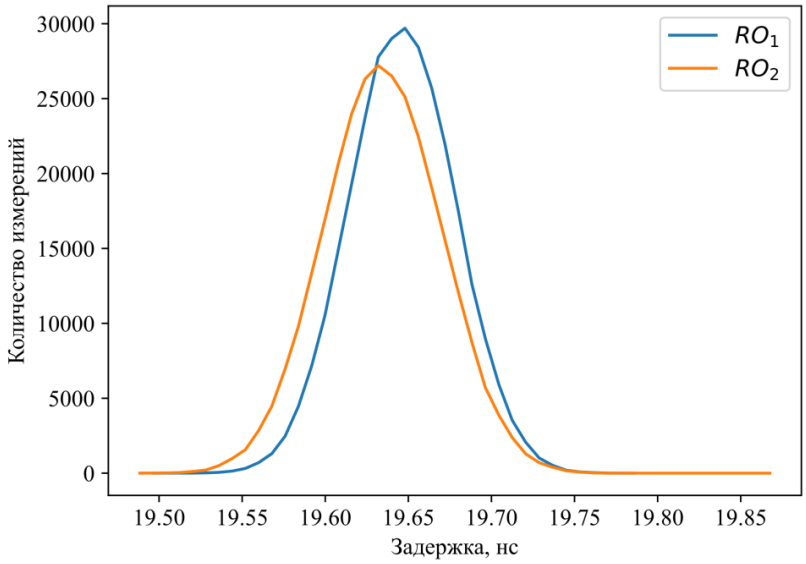

Рисунок 4 – Временное распределение задержек для конфигурации *N*=256 с управляемой линией задержки

Результаты свидетельствуют о состоятельности предложенного подхода к построению симметричных путей АФНФ. Рассчитанные характеристики стабильности и случайности имеют схожие значения с АФНФ той же разрядностью запроса, но построенных по классической схеме, и значительно более высокие значения межкристальной уникальности (0,27 и 0,02 соответственно) и при меньших аппаратурных затратах. Однако при условии использования D-триггера как арбитра сравнительно небольшая временная разница между минимальным и максимальным измеренными задержками может свидетельствовать о потенциальном нарушении условий предустановки и удержания его входных сигналов.

Список использованных источников:

1. Pappu, R. Physical One-Way Functions: PhD Thesis in Media Arts and Sciences / R. Pappu. – Cambridge : Massachusetts Institute of Technology, 2001. – 154 p.

2. Ярмолик, В. Н. Физически неклонируемые функции / В. Н. Ярмолик, Ю. Г. Вашинко // Информатика. – 2011. – № 2 (30). – С. 92–103.

3. Иванюк, А. А. Физическая криптография и защита цифровых устройств / А. А. Иванюк, С. С. Заливако // Доклады БГУИР. – 2019. – № 2 (120). – С. 50–58.

.

CONFIGURATION OF SYMMETRIC PATHS OF ARBITER PHYSICALLY UNCLONABLE FUNCTION ON FPGA

Shamyna A.Yu.

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

Ivaniuk A.A. – D. Sc. (Technology)

Annotation. The paper considers the synthesis of symmetrical paths of a physically non-cloneable function of the arbiter type, built on the basis of links, each of which functionally represents two repeaters, which are implemented on the basis of the LUT6 components of one FPGA slice block. A method for eliminating the asymmetry of interconnections based on controlled delay lines is described. The time characteristics of the symmetrical paths of the proposed structure are calculated for several configurations

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