ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК ФИЗИЧЕСКИ НЕКЛОНИРУЕМОЙ ФУНКЦИИ ТИПА АРБИТР НА ПЛАТАХ БЫСТРОГО ПРОТОТИПИРОВАНИЯ

Шамына А. Ю., Иванюк А. А.
Кафедра программного обеспечения информационных технологий, кафедра информатики, Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: shamyna@bsuir.by, ivaniuk@bsuir.by

В настоящей работе проведено исследование характеристик физически неклонируемых функциий типа арбитр, реализованных на ПЛИС. Описана реализация экспериментальной установки и технология сбора данных. Проведено сравнение характеристик с различными длинами симметричных путей

Введение

Физически неклонируемые функции (ФНФ) широко используются для защиты цифровых устройств от нелегального копирования, а также в качестве примитивов для генерации случайных числовых последовательностей. Особый интерес для исследования представляют ФНФ типа арбитр (АФНФ)[1], реализованные на FPGA, благодаря гибкости конфигурации и небольшим аппаратным затратам. Стабильность, случайность и уникальность являются важнейшими характеристиками ФНФ. Значения этих характеристик выступают в качестве критериев возможности использования ФНФ в определенных практических применениях. В данной работе проведено исследование характеристик АФНФ на нескольких платах быстрого прототипирования Digilent Nexys-4 с FPGA Artix-7[2].

I. Подготовка эксперимента и сбор данных

Реализация АФНФ предполагает наличие нескольких компонентов: генератор тестовых импульсов, блок симметричных путей (БСП) и схему арбитра. Схематично АФНФ представлена на рис. 1.

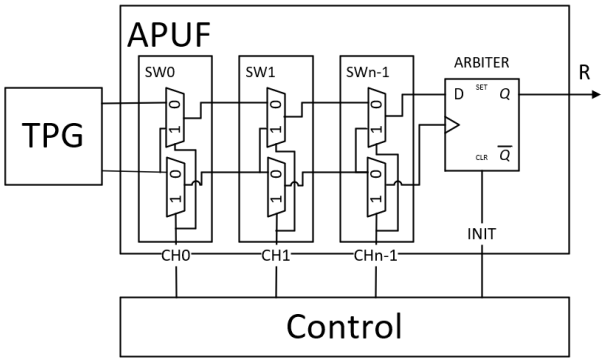

Рис. 1 – АФНФ типа арбитр

Проектное описание АФНФ было создано на языке VHDL с использованием САПР Vivado 2018.2. Передача данных между ПК и ПЛИС реализована на основе использования стандартных IP-компонент в среде Vivado. Также для проведения экспериментов и передачи данных через интерфейс UART на FPGA был развернут софт-процессор Microblaze[3], что позволило реализовать передачу данных между ПК и ПЛИС более эффективно. Программирование софт-процессора осуществлялось при помощи средств Xilinx SDK. Контроллер АФНФ был создан на основе цифрового конечного автомата (ЦКА).

Т.к. основной целью проведения эксперимента было исследование зависимости характеристик АФНФ от длины симметричных путей, было принято решение расположить арбитры через каждые 8 звеньев БСП. Благодаря этому стало возможным за один эксперимент получить результаты для АФНФ с различными длинами БСП. В данной реализации было выбрано число звеньев БСП $N = 128$. В качестве арбитра использован D-триггер.

Для генерации слабокоррелированных запросов использовался LFSR с внешними сумматорами по модулю два и характеристическим полиномом $\Phi(X) = x^{128} + x^{28} + x^{26} + x^2 + 1$. LFSR был реализован аппаратно, т.к. генерация запросов на стороне ПК и последующая их парадача на ПЛИС может значительно увеличить время эксперимента.

Для вычисления характеристик АФНФ было проведено $E = 10$ экспериментов на $M = 2$ различных кристаллах. В рамках каждого эксперимента было сгенерировано $C = 10^6$ псевдослучайных запросов. Для чтения данных из COM-порта на ПК и их записи в файлы использовалось ПО Tera Term. Также для анализа полученных результатов было реализовано собственное программное средство на языке программирования C#, включающее в себя функции по анализу стабильности и случайности ответов ФНФ.

II. Исследование характеристик АФНФ

Стабильность является одной из ключевых характеристик ФНФ. Для классической реализации АФНФ свойственны метастабильные от-

веты на определенные запросы, которые возникают из-за перехода схемы арбитра в метастабильное состояние при минимальной разнице между фронтами тестовых сигналов. Это может негативно сказаться на стабильности ответов и требовать применения дополнительных решений. Для экспериментальной оценки стабильности был использован подход, описанный в работе [4].

Результаты по измерению средней стабильности S_{avg} для АФНФ различной разрядности, полученные в результате эксперимента, показаны на рисунке 2.

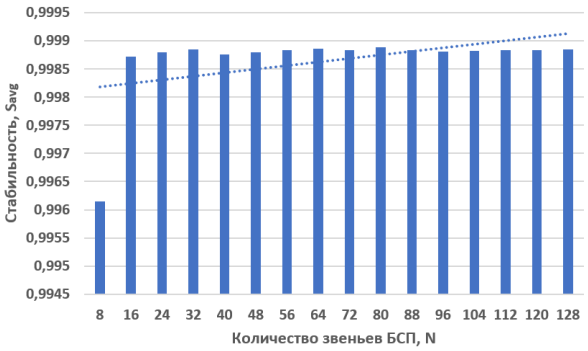

Рис. 2 – Зависимость значения средней стабильности АФНФ от количества пар мультиплексоров

Минимальное значение стабильности составляет $S_{min} = 0.5$ для каждой из реализаций. Доли метастабильных ответов от общего числа представлены на рисунке 3. Полученные результаты демонстрируют увеличение стабильности с увеличением длины симметричных путей.

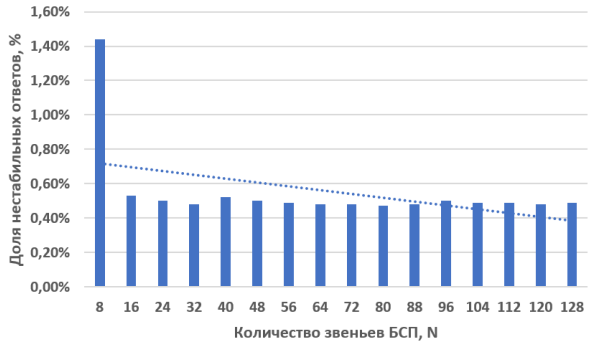

Рис. 3 – Зависимости доли метастабильных ответов АФНф от количества пар мультиплексоров

Для оценки случайности была взята вероятность появления ответа $r = 1$. Пусть ФНФ сгенерировала последовательность ответов R длиной n, тогда для оценки вероятности появления символа α p_α, встретившегося в R ровно k_α раз является отношение:

$$p_\alpha = \frac{k_\alpha}{n}.$$

Таким образом, рассчитанные результаты p_1 отображены в виде гистограммы на рисунке 4.

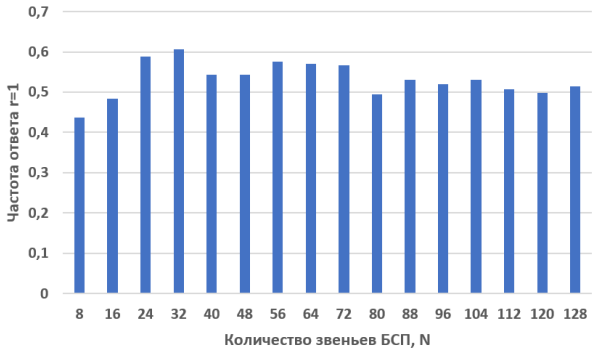

Рис. 4 – Зависимость значения вероятности ответа АФНФ $r = 1$ от количества пар мультиплексоров

Полученные результаты свидетельствуют о стабилизации значения p_1 к эталонному $p_1 = 0.5$ при увеличении количества звеньев БСП.

III. Заключение

В ходе экспериментального исследования АФНФ различной размерности были оценены такие характеристики ФНФ, как стабильность и случайность. На основе полученных данных можно сделать вывод об улучшении характеристик ФНФ с увеличением длины БСП. Однако с увеличением длины БСП возрастают аппаратные затраты и время отклика, что может являться существенным ограничением в определенных случаях.

Также при анализе результатов были обнаружены нестабильные ответы для определенных запросов. Это может затруднить использование классической реализации АФНФ в случаях, где требуется высокая стабильность.

В дальнейших исследованиях планируется изучить подходы по увеличению стабильности АФНФ, а также влияние динамических эффектов на характеристики ФНФ.

Список литературы

1. A technique to build a secret key in integrated circuits for identification and authentication applications / J.W. Lee [et al.] // Intern. Symp. VLSI Circuits (VLSI'04), Honolulu, USA, June 15–19, 2004. – Honolulu, 2004. – P. 176–179
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, 2020. — Date of access: 30.10.2020.
3. Microblaze soft processor core [Electronic resource]. — Mode of access: https://www.xilinx.com/products/design-tools/microblaze.html. — Xilinx, Inc, 2020. — Date of access: 30.10.2020.
4. Метод увеличения стабильности физически неклонируемой функции типа арбитр. / Заливако С.С., Иванюк А.А., В.П. Клыбик // Информатика – 2017. – №1(53) С. 31-43.