# ПРОБЛЕМА РЕАЛИЗАЦИИ СИММЕТРИЧНЫХ ПУТЕЙ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ ТИПА АРБИТР НА ПРОГРАММИРУЕМЫХ ЛОГИЧЕСКИХ ИНТЕГРАЛЬНЫХ СХЕМАХ

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

*В работе обозначены проблемы реализации физически неклонируемых функций типа арбитр на программируемых логических интегральных схемах (ПЛИС), связанные с соблюдением условия симметрии для пар реконфигурируемых путей. Проанализированы задержки на уровнях коммутационных элементов и их соединений. Приведены решения проблемы построение симметричных пар путей АФНФ на ПЛИС*

## Введение

Повсеместное использование информационных технологий, возрастающие требования к обеспечению безопасности их использования определяют актуальность разработки соответствующих средств защиты. Актуальным является использование физической криптографии, основанной на структурной сложности и невоспроизводимости некоторых параметров и характеристик физических систем. В области физической криптографии распространено использование физически неклонируемых функций (ФНФ) [1].

ФНФ является структурой, позволяющей отображать множество запросов $CH$ во множество ответов $R$ уникальным и невоспроизводимым образом $CH \rightarrow R$. В цифровых устройствах преобладает использование ФНФ, базирующихся на уникальности и невоспроизводимости задержек распространения сигналов через их пути. Одним из таких типов ФНФ является ФНФ типа арбитр (АФНФ) [2-4].

Путь цифрового устройства представляется как группа последовательно подключенных элементов и их соединений, имеющая единственный вход и единственный выход. Фундаментальным условием функционирования АФНФ является формирование множества ответов $R$ на основе уникальных задержек множества пар симметричных путей. Задержки распространения сигналов через пару путей $A$ и $B$ ($t^A_{pd}$ и $t^B_{pd}$) сформированы случайной $t^A_{pd_r}$, $t^B_{pd_r}$ и статической составляющими $t^A_{pd_s}$ и $t^B_{pd_s}$.

Случайные составляющие невозможно оценить до производства конкретного экземпляра цифрового устройства, а статические составляющие определяются на этапе проектирования.

Использование программируемых логических интегральных схем (ПЛИС) в качестве платформы для реализации цифровых устройств, поставляемых потребителю, определяет для них актуальность использования средств защиты. Реализация АФНФ на ПЛИС связана со сложностью соблюдения условия симметрии для множества пар путей. Если имеется некая пара путей $A$ и $B$, тогда условие симметрии определяется как $|t^A_{pd_s} - t^B_{pd_s}| \rightarrow 0$.

В случае несоблюдения этого условия для пар путей АФНФ наблюдается ухудшение характеристик случайности и уникальности [2-4], что часто приводит к невозможности использования АФНФ.

## I. Реализация АФНФ

Структурная схема АФНФ представлена на рисунке 1. В ней можно выделить генератор тестового импульса (ГТИ), блок реконфигурируемых симметричных путей (БСП) и арбитр (АРБ).

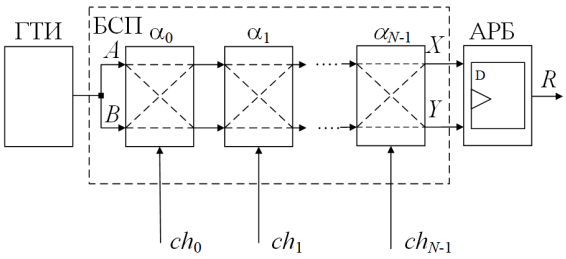


Рис. 1 – Структурная схема АФНФ

Одно звено реконфигурируемых путей АФНФ $\alpha_i$, $i \in [0; N\text{-}1]$ представляет собой структуру, имеющую два входа и два выхода, обеспечивающую прямую либо перекрестную коммутацию сигналов со входов на выходы в зависимости от значения запроса $ch_i$. Как известно, такая структура может быть построена с использованием двух двухвходовых мультиплексоров и в случае ПЛИС типа FPGA реализуется на технологических элементах LUT. Это приводит к асимметрии путей распространения сигналов в рамках одного звена $\alpha_i$ (рисунок 2) и их соединений.

Работа выполнена в совместной учебной лаборатории БГУИР-YADRO
https://www.bsuir.by/ru/kaf-informatiki/yadro

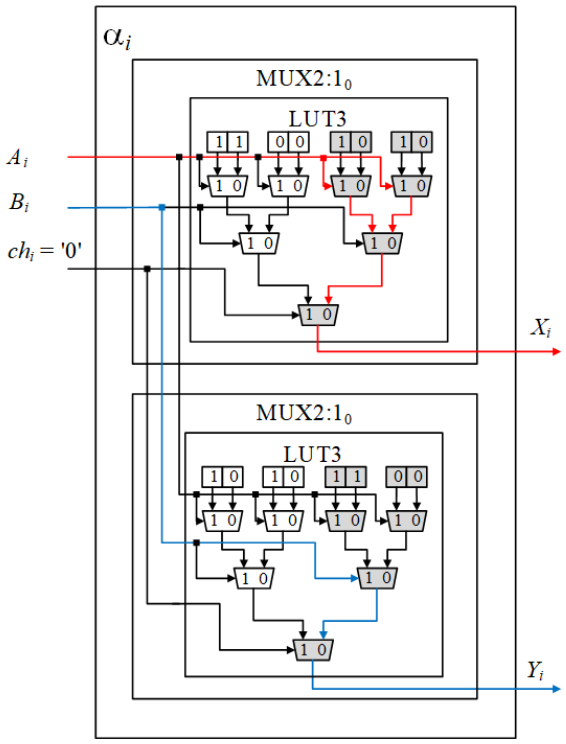


Рис. 2 – Схема звена реконфигурируемых путей АФНФ

Как видно из рисунка 2, исходя из внутренней структуры технологических компонентов LUT3, сигнал с входов $A_i$ и $B_i$ на выходы $X_i$ и $Y_i$ проходит через разное количество мультиплексоров внутри LUT, что определяет разные значения задержек распространения сигналов. В работе [3] проводится экспериментальное исследование задержек реконфигурируемых путей АФНФ $A$ и $B$. Полученные результаты демонстрируют разницу математических ожиданий $\Delta(\mu_A,\mu_B,) = 190$пс, что может свидетельствовать о нарушении условия симметрии при синтезе реконфигурируемых путей. Для анализа асимметрии реконфигурируемых путей АФНФ в настоящей работе рассматривается асиметрия их коммутационных звеньев и соединений.

При автоматическом синтезе реконфигурируемых путей АФНФ наблюдается асимметрия распространения сигналов через их коммутационные звенья из-за неконтролируемого сопоставления информационных входов мультиплексоров с физическими входами LUT. При использовании технологических элементов LUT6 из серии ПЛИС Xilinx Artix-7 для реализации двухвходового мультиплексора возможны 120 вариантов конфигурации LUT. В работе [2] проведены экспериментальные исследования задержек таких конфигураций. Ввиду особенностей используемой схемы анализа задержек наиболее показательной статистической характеристикой, демонстрирующей временные различия задержек конфигураций LUT является среднеквадратичное отклонение*.

Экспериментальный анализ задержек соединений технологических блоков реконфигурируемых путей АФНФ невозможен без существенной модификации их структуры. Поэтому для этой цели для $N = 128$ была создана параметрическая модель. Статистические оценки задержек (математическое ожидание $\mu$, среднеквадратичное отклонение $\sigma$ и их отношение) коммутационных элементов и их соединений приведены в таблице 1.

Таблица 1 – Статистические характеристики задержек реконфигурируемых путей АФНФ

| Характеристика | Коммутационные элементы | Соединения |
|---|---|---|
| $\mu$ | 1369 пс* | 563,33 пс |
| $\sigma$ | 3,8 пс | 287,9 пс |
| $\sigma$ / $\mu$ | 0,003 | 0,513 |

## II. Решения проблемы реализации симметричных пар путей АФНФ на ПЛИС

Для решения проблемы построения пар симметричных путей АФНФ могут применяться различные по своей сути и реализации методы. К ним относят: методы балансировки задержек путей с использованием управляемых линий задержки [2], методы на основе временных оценок задержек сигналов путей с возможностью автоматической реализации [3]. Либо использоваться альтернативные подходы к созданию пар симметричных путей, например, на основе перестановочных сетей с соблюдением условия симметрии за счет особенностей синтеза сложноструктрных элементов на ПЛИС [4].

## III. Заключение

Полученные результаты свидетельствуют о наличии разниц статических составляющих задержек при реализации АФНФ на ПЛИС как на уровне коммутационных звеньев реконфигурируемых путей, так и на уровне их соединений. Причем, разница задержек на уровне соединений больше на несколько порядков разницы коммутационных элементов. Эти факты являются показателями нарушения условия симметрии пар путей и подтверждают необходимость использования альтернативных способов их синтеза на ПЛИС.

## IV. Список литературы

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. Шамына, А. Ю. Построение и балансировка путей физически неклонируемой функции типа арбитр на FPGA / А. Ю. Шамына, А. А. Иванюк // Информатика. – 2022. – Т. 19, № 4. – С. 27–41.
3. Шамына, А. Ю. Автоматическая балансировка путей физически неклонируемой функции типа «арбитр» / А. Ю. Шамына, А. А. Иванюк // Доклады БГУИР, 2023. – Т. 21, № 3. – С. 56–62
4. Иванюк, А. А. Физически неклонируемая функция типа абитр с нелинейными парами путей / А. А. Иванюк, А. Ю. Шамына // Системный анализ и прикладная информатика. – 2023. – № 1. – С. 54–62.