ОТЗЫВ

на диссертационную работу **Шамыны Артёма Юрьевича**
на тему «Методы и средства балансировки путей физически неклонируемых функций типа арбитр, реализованных на программируемых логических интегральных схемах», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.05 – «элементы и устройства вычислительной техники и систем управления»

Диссертационная работа Шамыны А. Ю. посвящена решению актуальной научно-технической задачи разработки методов и средств балансировки путей физически неклонируемых функций типа арбитр (АФНФ), реализованных на программируемых логических интегральных схемах (ПЛИС).

Актуальность исследования определяется необходимостью разработки средств неклонируемой идентификации и генераторов случайных числовых последовательностей, требующих аппаратных решений с высокими характеристиками уникальности и случайности. Классические АФНФ, реализуемые на ПЛИС, подвержены асимметрии конфигурируемых элементов и межсоединений, возникающей при автоматизированном синтезе, что приводит к низким значениям межкристальной уникальности и единообразия, неприемлемым для практического применения. Разработка методов балансировки пар путей АФНФ на ПЛИС, обеспечивающих выполнение условия их симметрии и позволяющих достичь значений межкристальной уникальности и единообразия, сопоставимых с реализациями на заказных сверхбольших интегральных схемах (СБИС), представляет собой актуальную научно-техническую задачу.

В диссертации решён комплекс взаимосвязанных задач, включающий:

– разработку метода автоматизированного синтеза балансируемых путей АФНФ на основе управляемых линий задержек с использованием априорной информации о технологических элементах ПЛИС;

– разработку архитектуры АФНФ с возможностью автоматической балансировки пар путей, основанной на анализе их временных характеристик;

– разработку алгоритма коррекции формирования ответа АФНФ, основанного на оценке временных характеристик множеств пар путей;

– разработку метода синтеза путей АФНФ, основанного на особенностях реализации схем перестановочных сетей, с целью автоматического обеспечения симметрии этих путей на ПЛИС.

В ходе исследования Шамына А. Ю. получил следующие результаты:

– разработан метод автоматизированного синтеза балансируемых пар путей АФНФ на ПЛИС, заключающийся в построении симметричных звеньев путей с фиксированным сопоставлением физических и логических входов LUT-блоков, применении двухступенчатых программируемых линий задержек и определении конфигураций этих линий, обеспечивающих

минимально возможное абсолютное значение оценки математического ожидания разности задержек пар путей;

– разработан метод автоматической балансировки задержек пар путей АФНФ на ПЛИС, заключающийся в преобразовании блока симметричных путей в пару конфигурируемых кольцевых осцилляторов, применении модифицированного арбитра, сравнивающего значения счетчиков импульсов, формируемых этими осцилляторами в заданном окне измерений, и расчете корректирующего значения в режиме обучения для его учета при формировании бита ответа в нормальном режиме;

– разработан метод синтеза элементов перестановочных сетей, позволяющий коммутировать все возможные пары путей; применение данного метода при синтезе схем АФНФ повышает линейную сложность формируемых ответов и автоматически компенсирует асимметрию конфигурируемых пар путей.

Практическая значимость работы подтверждена внедрением разработанных методов балансировки путей физически неклонируемых функций типа арбитр в процесс проектирования микроконтроллеров твердотельных накопителей компании-резидента Парка высоких технологий – ООО «СК Хайникс Мемори Солюшнс Восточная Европа». Применение данных методов позволяет минимизировать негативные эффекты асимметрии пар путей АФНФ как при автоматизированном синтезе, так и при временной деградации кристаллов, что значительно улучшает характеристики АФНФ и делает возможным их использование в протоколах аутентификации цифровых устройств. Результаты диссертационного исследования также внедрены в учебный процесс учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» по специальностям магистратуры 1-40 80 05 «Программная инженерия» и 1-40 80 05 «Программное обеспечение информационных технологий» в рамках лекционных курсов и лабораторных работ по дисциплинам, связанным с проектированием аппаратных средств защиты информации и генераторов случайных числовых последовательностей. Внедрение разработанных методов в образовательный процесс позволяет формировать у студентов навыки практического применения методов физической криптографии, проектирования физически неклонируемых функций и их реализации на ПЛИС, а также использования современных подходов к обеспечению информационной безопасности аппаратных платформ.

В процессе работы над диссертацией Шамына А. Ю. проявил высокий уровень самостоятельности, глубокое понимание принципов проектирования аппаратных средств защиты цифровых устройств, ответственность и умение решать научно-технические задачи.

На основании изложенного считаю, что диссертационная работа Шамыны Артёма Юрьевича представляет собой завершённое научное исследование, а её автор заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.05 – «Элементы и устройства

вычислительной техники и систем управления» за новые научно обоснованные результаты:

1. Метод автоматизированного синтеза балансируемых путей АФНФ, использующий управляемые линии задержки и априорную информацию о технологических элементах ПЛИС, улучшающий по сравнению с классическим способом построения путей значения характеристик межкристальной уникальности с 0,012 до 0,484 и единообразия с 0,968 до 0,999 для ПЛИС Xilinx Artix-7.

2. Двухступенчатая схема балансировки пар путей 128-разрядной АФНФ на основе программируемых элементов задержки, позволяющая снизить абсолютное значение оценки математического ожидания разности задержек пар путей с 124 до 0,2 пс для ПЛИС Xilinx Artix-7.

3. Метод автоматической балансировки пар путей АФНФ, основанный на оценке их временных характеристик, улучшающий по сравнению с классическим способом построения путей значения характеристик межкристальной уникальности с 0,012 до 0,449 и единообразия с 0,968 до 0,995 для ПЛИС Xilinx Artix-7.

4. Метод синтеза сбалансированных путей АФНФ, основанный на реализации схем перестановочных сетей на ПЛИС, автоматически улучшающий по сравнению с классическим способом построения путей значения характеристик межкристальной уникальности с 0,012 до 0,437 и единообразия с 0,968 до 0,987 для ПЛИС Xilinx Artix-7.

5. Архитектуры блоков симметричных путей, основанные на модифицированных элементах перестановочных сетей, обеспечивающие автоматическую балансировку пар путей АФНФ и снижение абсолютного значения оценки математического ожидания разности задержек пар путей с 124 до 24 пс для 128-разрядной АФНФ на SoC Xilinx Zynq-7000.

Научный руководитель
профессор кафедры информатики БГУИР,
доктор технических наук, профессор

29.09.2026 Иванюк А.А

ПОДПИСЬ УДОСТОВЕРЯЮ
Начальник центра кадровой работы
(подпись, ФИО)
29 09 2026 г.