ОТЗЫВ

на автореферат диссертации Прудникова Вадима Александровича выполненной на тему «Синтез и исследование псевдо-динамических подстановок» и представленной на соискание ученой степени кандидата технических наук по научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность»

Разработка высокопроизводительных и надёжных криптографических алгоритмов остаётся ключевой проблемой в сфере информационной безопасности. Особую значимость эта задача приобретает в условиях, когда к программным реализациям предъявляются строгие требования по быстродействию и потребляемым вычислительным ресурсам, особенно для устройств с ограниченными вычислительными возможностями. В данном аспекте представленный в работе подход к синтезу псевдо-динамических подстановок с использованием ARX-конструкций является весьма перспективным и соответствует современным запросам.

Научная новизна диссертационного исследования заключается в разработке метода синтеза PD-sbox-ARX, обеспечивающего минимизацию потребления вычислительных ресурсов при сохранении сопоставимой криптографической стойкости, что подтверждается как теоретическими выкладками, так и экспериментами.

В автореферате представлены убедительные доказательства состоятельности предложенной псевдо-динамической подстановки и метода их синтеза, включая формальные модели и сравнительный анализ с существующими аналогами. Достоверность результатов подкреплена экспериментальными данными, оценивающими ключевые параметры: показатели нелинейности, устойчивость к дифференциальному криптоанализу, эффективность работы на различных платформах.

Практическая значимость исследования заключается в возможности применения разработанного метода при разработке криптографических компонентов для программных систем защиты данных. Полученные результаты открывают перспективы для модернизации алгоритмов шифрования, используемых в распространённых протоколах безопасности типа SSH и TLS.

Автореферат написан научным языком, выдержанным в соответствии с требованиями к диссертационным работам. Структура документа логична: постановка задачи, анализ существующих решений, изложение предложенного подхода, описание результатов и заключение. Материал изложен последовательно, с достаточной детализацией, позволяющей оценить научную и практическую значимость работы.

По содержанию автореферата, следует обратить внимание на отдельные недостатки диссертационной работы:

1. Из текста автореферата ясно, что автором представлена и проанализирована программная реализация псевдо-динамической подстановки PD-sbox-ARX на

различных архитектурах микроконтроллеров. Было бы интересно рассмотреть вопрос практического применения PD-sbox-ARX на ПЛИС.

2. В тексте автореферата упоминается фреймворк CASCADA, однако описание его применение недостаточно.

Отмеченные недостатки не относятся к вопросам, выносимых на защиту, и не влияют на положительную оценку автореферата и собственно диссертационной работы.

Диссертация Прудникова Вадима Александровича «Синтез и исследование псевдо-динамических подстановок» удовлетворяет требованиям, установленным Положением «О присуждении учёных степеней в федеральном государственном автономном образовательном учреждении высшего образования «Южный федеральный университет» (в действующей редакции) и предъявляемым к диссертациям на соискание учёной степени кандидата наук, а автор, Прудников Вадим Александрович, заслуживает присвоения ему учёной степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность», технические науки.

Ожиганова Марина Ивановна,
кандидат технических наук,
заведующий кафедрой
«Информационная безопасность»
Севастопольского
государственного университета
299033, г. Севастополь, ул.Курчатова, 7

Подпись Ожигановой М.И. удостоверяю
Начальник отдела кадров
С.В. Бернацкая
«05» 06 2025 г.