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»

Актуальность диссертационного исследования Прудникова В.А. определяется важностью задачи синтеза криптографических подстановок, удовлетворяющих заданным требованиям. Однако зачастую эти требования оказываются противоречивыми. Указанная проблема оказывается значимой при разработке эффективных псевдослучайных функций (PRF) и псевдослучайных перестановок (PRP), играющих ключевую роль в современных криптографических системах. Разработка теоретических основ и практических методов синтеза псевдо-динамических подстановок в этих условиях представляет собой актуальную научную проблему, имеющую существенное значение для развития современных криптографических технологий.

Основным научным вкладом автора является разработка универсального метода синтеза псевдо-динамических подстановок на основе ARX-функций, позволяющего путём подбора параметров ARX-функций минимизировать количество затрачиваемых ассемблерных инструкций на операции циклического сдвига при их реализации на малоресурсных 8-битных микроконтроллерах архитектуры AVR. В тексте автореферата представлены обоснования корректности разработанных алгоритмов и методов, включающие: формальные математические модели, сравнительный анализ с существующими криптографическими решениями. Экспериментальная часть исследования содержит комплексную верификацию ключевых параметров: уровень нелинейности, показатели дифференциальной стойкости, эффективность реализации на различных вычислительных архитектурах. Полученные эмпирические данные подтверждают надёжность и обоснованность сделанных выводов, что свидетельствует о достоверности представленных результатов. Предложенный универсальный метод синтеза псевдо-динамических подстановок на основе ARX-функций применим для проектирования криптографических примитивов в программных средствах защиты информации.

Автореферат диссертационного исследования составлен в соответствии с действующими нормативными требованиями. Документ обладает чёткой структурой, включающей все необходимые компоненты. Материал изложен последовательно, с достаточной детализацией, позволяющей оценить научную и практическую значимость работы.

Работа заслуживает положительной оценки, однако хочется обратить внимание, что автор практически не затронул вопрос переноса технологии на перспективные ЭВМ с большей длиной машинного слова.

В целом, диссертационная работа 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 её 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.

Аршинский Леонид Вадимович,
доктор технических наук, доцент, профессор кафедры «Информационные системы и защита информации» ФГБОУ ВО «Иркутский государственный университет путей сообщения».
Адрес: 664074, Иркутская обл., г. Иркутск, ул. Чернышевского, 15.
e-mail: arshinsky_lv@irgups.ru,
телефон: 8(3952) 638-359

09.06.2025

Подпись Аршинского Л.В.
ЗАВЕРЯЮ:
Начальник общего отдела ИрГУПС
Подпись
«09» 06 2025 г.