**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»

Криптографические подстановки sbox служат ключевым нелинейным элементом многих современных псевдослучайных функций (PRF) и псевдослучайных перестановок (PRP). Их нелинейные свойства во многом определяют устойчивость криптографической функции к криптоанализу. Стоит отметить, что sbox — один из самых затратных элементов с точки зрения вычислительных ресурсов, будь то программная или аппаратная реализация. Поскольку криптографические алгоритмы используют итеративную структуру, характеристики sbox напрямую влияют на требуемое число раундов, потребляемые вычислительные ресурсы, скорость обработки блока и энергопотребление.

Актуальность исследований в области синтеза криптографических подстановок высока: создание sbox, отвечающих жёстким и противоречивым требованиям, — основа для разработки эффективных PRF/PRP. PRF в AEAD-режимах (например GCM) демонстрируют более высокую производительность, чем блочные шифры, и широко применяются в протоколах SSH, TLS, OpenVPN. Внедрение псевдо-динамических подстановок на основе ARX-функций при построении PRF потенциально может привести к увеличению криптографической стойкости, без ущерба эффективности программной реализации. Синтез и анализ подобных криптографических примитивов — перспективное направление, обладающее практической и научной ценностью.

Достоверность результатов и обоснованность научных положений, результатов и основных выводов диссертационной работы подтверждается сходимостью исходной гипотезы с результатами опытно-экспериментальных данных, а также строгостью применяемого математического аппарата.

Теоретическая значимость результатов исследования состоит в развитии перспективного научного направления синтеза и применения псевдо-динамических подстановок на основе ARX-функций, удовлетворяющих широкому спектру противоречивых требований по стойкости к криптоанализу и затрачиваемым

Применение псевдо-динамических подстановок на базе подобранных ARX-функций, обладающих дифференциальными и линейными свойствами эквивалентных подстановок, аналогичными случайно сформированным фиксированным подстановкам той же размерности, позволяет обеспечить критический путь (максимальное количество последовательных операций сложения по модулю $2^{16}$) в четыре раза меньше, чем 8-итерационная 32-битная Alzette-подобная структура, при двухкратном увеличении количества операций и при сопоставимых максимальных значениях весов разностных и линейных характеристик. При аппаратной реализации ARX-функции данное свойство позволяет пропорционально уменьшить (до 4 раз) задержку при преобразовании блоков информации.

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, можно указать на отдельные недостатки работы:

1. Из текста автореферата не ясно, рассмотрено ли в диссертационной работе применение разработанного криптографического примитива PD-sbox-ARX в составе псевдослучайных функций (PRF) и/или псевдослучайных перестановок (PRP) и проведён ли их анализ. Продемонстрировало ли применение PD-sbox-ARX улучшение криптографических характеристик результирующих конструкций и если да, то каких?
2. В автореферате рисунок 2, на котором представлена псевдо-динамическая подстановка PD-sbox_4x64x64, недостаточно читаем.

Отмеченные недостатки не влияют на положительную оценку автореферата и собственно диссертационной работы.

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 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.

Дахкильгова Камила Багаудиновна,
кандидат технических наук, и.о. заведующего кафедрой программирования и инфокоммуникационных технологий, и.о. директора института математики, физики и информационных технологий ФГБОУ ВО «Чеченский государственный университет им. А.А. Кадырова»

Почтовый адрес:
364024, г. Грозный, ул. Шерипова, 32

Заверяю подпись Дахкильговой К.Б.
Начальник отдела кадров персонала Шаломаева Т.
(подпись) (расшифровка)