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 являются основным нелинейным элементом множества современных псевдослучайных функций (PRF) и псевдослучайных перестановок (PRP). Нелинейность данного криптографического примитива напрямую влияет на сложность криптоанализа функции в целом. Подстановки sbox являются одним из наиболее ресурсоёмких элементов при их программной или аппаратной реализации. Так как криптографические функции строятся по итеративной схеме, от нелинейных свойств фиксированных подстановок напрямую зависит количество итераций, затрачиваемых вычислительных ресурсов, а также время обработки и потребляемая мощность. К фиксированным операциям подстановки предъявляется множество противоречивых требований, влияющих на криптографическую стойкость. Для малоресурсных алгоритмов особо актуальна защита от побочных каналов, накладывающая дополнительные ограничения.

Актуальность исследований в области синтеза криптографических подстановок высока: создание sbox, отвечающих жестким 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 полученных результатов

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 ресурсам при программной реализации криптографических преобразований.

Практическая ценность полученных результатов

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. В содержании работы некоторые абзацы излишне перегружены техническими терминами (например, описание PD-sbox_4x64x64), что затрудняет восприятие автореферата;
2. В автореферате рисунок 2, на котором представлена псевдо-динамическая подстановка PD-sbox_4x64x64, недостаточно читаем.

Отмеченные недостатки не относятся к вопросам, выносимых на защиту, и 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.

Филаретов Геннадий Федорович,
доктор технических наук, профессор, профессор кафедры управления и интеллектуальных технологий Московский энергетический институт (национальный исследовательский университет). Институт информационных и вычислительных технологий.

Почтовый адрес:
111250, г. Москва, Е-250, ул. Красноказарменная, 14.
FilaretovGF@mpei.ru; +79255176319.

Подпись удостоверяю

ЗАМЕСТИТЕЛЬ НАЧАЛЬНИКА УПРАВЛЕНИЯ ПО РАБОТЕ С ПЕРСОНАЛОМ
Л.И.ПОЛЕВАЯ