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 обусловлена тем, что центральным местом в современных криптографических примитивах – псевдослучайных функций (Pseudo Random Function – PRF) и псевдослучайных перестановок (Pseudo Random Permutation – PRP) выступают операции перестановки или замены (sbox). Будучи основным источником нелинейности за счет взаимно однозначного или не взаимно однозначного преобразования m-битного сообщения на входе в n-битное сообщение на выходе, подстановки (замены) sbox критически влияют на:

- сложность криптоанализа PRF/PRP;
- ресурсоемкость (время, мощность, вычисления) реализации, особенно в итеративных схемах;
- устойчивость к атакам по побочным каналам, что особенно важно для систем с ограниченными ресурсами.

Ключевой проблемой в данном случае является синтез sbox, который одновременно должен удовлетворять нескольким и зачастую взаимоисключающим требованиям криптостойкости и эффективности. Поскольку данная задача в настоящее время решена не полностью, то настоящее исследование актуально, так как фокусируется на псевдо-динамических подстановках. Их использование в PRF, включая высокоэффективные AEAD-режимы, вытесняющие блочные шифры в протоколах SSH/TLS/OpenVPN, может обеспечить превосходящую криптостойкость без увеличения затрат на реализацию, что открывает новые перспективы для криптографии.

Научная новизна диссертационного исследования заключается в следующем:

1. Разработана структура псевдо-динамической операции подстановки на основе ARX-функций, обладающая свойствами эквивалентных замен, аналогичными случайно сформированным операциям подстановки той же размерности (пункт 19 паспорта специальности).

2. Разработан и исследован метод синтеза параметров 32-битной ARX-функции, позволяющий получить параметры операций циклического сдвига, при которых обеспечивается максимальный вес разностной характеристики, равный 2^{-32} (эмпирический вес 2^{-26}), и вес линейной характеристики 2^{-13} для результирующего PD-sbox-ARX, включающей в свой состав четыре 32-битные ARX-функции, а также позволяющий минимизировать количество затрачиваемых ассемблерных

инструкций на операции циклического сдвига при реализации на малоресурсных 8-битных микроконтроллерах семейства AVR (пункт 19 паспорта специальности).

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.

Замечания и рекомендации

1. В тексте автореферата представлен универсальный метод синтеза PD-sbox-ARX, для микроконтроллеров семейства AVR, однако его важный начальный этап эвристического выбора структуры ARX-функции с учетом особенностей программной и аппаратной реализации, не формализован, что не позволяет понять, насколько он зависит от опыта и интуиции исследователя.
2. В тексте автореферата представлено сравнение разработанной подстановки PD-sbox-ARX с такими криптографическими преобразованиями, как miniAlzette32 (Alzette-подобная структура) и 8 раундов криптоалгоритма Speck32. Однако не ясно, проводилось ли сравнение PD-sbox-ARX с малоресурсными реализациями отечественных криптоалгоритмов «Кузнечик» или «Магма»? Если нет, то чем это аргументировано?

Выводы

Несмотря на указанные замечания, согласно автореферату, диссертационное исследование соответствует необходимому научно-техническому уровню и отвечает критериям специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность».

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.

Жук Александр Павлович кандидат технических наук, научная специальность 20.02.14 «Вооружение и военная техника. Комплексы и системы военного назначения», профессор, профессор кафедры организации и технологии защиты информации ФГАОУ ВО «Северо-Кавказский федеральный университет»

«06» июня 2025 г.

Почтовый адрес:
355017, г. Ставрополь, ул. Пушкина, д. 1.
Телефон: 8(8652)95-68-00, внутр. 53-38.
Электронная почта: azhuk@ncfu.ru.

ПОДПИСЬ
УДОСТОВЕРЯЮ
льник Управления
делами СКФУ
Логачева А. В.