ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

на диссертационную работу Прудникова Вадима Александровича на тему **«Синтез и исследование псевдо-динамических подстановок»**, представленную на соискание учёной степени кандидата технических наук по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность»

1. Актуальность темы диссертационного исследования

Операции замены или фиксированные подстановки sbox являются основным нелинейным элементом для множества современных псевдослучайных функций (Pseudo Random Function – PRF) и псевдослучайных перестановок (Pseudo Random Permutation – PRP), которые являются базовым элементом логической защиты информации в информационных системах. Под термином «подстановка» (sbox, замена) подразумевается как взаимно однозначное, так и не взаимно однозначное преобразование m-битного сообщения на входе в n-битное сообщение на выходе, где n не всегда равно m.

Нелинейность подстановок напрямую влияет на сложность криптоанализа псевдослучайных функций и псевдослучайных перестановок, операции замены являются одним из наиболее ресурсоёмких элементов при программной или аппаратной реализации. Так как PRF и PRP строятся по итеративной схеме (для достижения заданного уровня суммарной нелинейности преобразования), от нелинейных свойств фиксированных подстановок напрямую зависит количество итераций, затрачиваемых вычислительных ресурсов, а также время обработки и потребляемая мощность.

К фиксированным операциям подстановки предъявляется около десятка требований, напрямую влияющих на криптографическую стойкость PRF и PRP. Для малоресурсных псевдослучайных функций и псевдослучайных перестановок остро встаёт проблема защиты от побочных каналов утечки секретной информации. Это накладывает дополнительные требования и ограничения на подстановки.

Актуальность исследований заключается в том, что проблема синтеза подстановок, удовлетворяющих широкому спектру взаимоисключающих требований, является базовой при синтезе эффективных PRF и PRP. Псевдослучайные функции, работающие в режиме счётчика с аутентификацией Галуа (Authenticated Encryption with Associated Data – AEAD), в большинстве случаев способны заменить современные блочные шифры, например, в протоколах SSH и TLS, а также OpenVPN, так как обладают более высокой производительностью и/или меньшим потреблением ресурсов при программной реализации. Однако применение псевдо-динамических подстановок при синтезе PRF потенциально способно обеспечить устойчивость к криптоанализу превосходящую аналоги, при сохранении сопоставимых затратах ресурсов при программной реализации. Следовательно, синтез и исследование псевдо-динамических подстановок является актуальной темой и представляет научный и практический интерес.

2. Оценка достоверности полученных результатов и новизны диссертационного исследования

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.

Научная новизна состоит 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 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 работы:

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.

3. Оценка содержания диссертации, степени её завершённости, подтверждение публикаций автора

Содержание и структура диссертации Прудникова В. А. соответствуют теме, целям и задачам исследования. Диссертация написана на русском языке, состоит из введения, трёх глав, заключения, списка используемых источников из 71 наименования и приложения. Полный объём диссертации составляет 133 страницы (в том числе приложения – 7 страниц), включая 31 рисунок, 28 таблиц. Структура диссертации логичная, рисунки и таблицы оформлены в соответствии со стандартами ГОСТ.

Во введении обосновывается актуальность темы, формулируются научная задача исследования, определяются объект и предмет исследования, практическая ценность и научная новизна результатов, излагаются научные положения, выдвигаемые на защиту.

В первой главе содержится анализ существующих подходов к синтезу псевдо-динамических операций подстановки. Приводится анализ синтеза операций подстановки, как основного нелинейного элемента современных блочных шифров и

псевдослучайных функций. Даётся описание структуры псевдо-динамической операции подстановки PD-sbox, линейный и дифференциальный криптоанализ PD-sbox на основе фиксированных операций подстановки. Представлено описание метода автоматизированного поиска криптографических характеристик с использованием SMT решателей и библиотеки CASCADA. Приведены выводы о том, что существующие подходы к синтезу и применению динамических операций подстановки не позволяют одновременно обеспечить стойкость, минимизацию затрачиваемых ресурсов и скорость программной реализации псевдослучайных функций на их основе, сопоставимую с псевдослучайными функциями на основе фиксированных подстановок. В связи с этим синтез псевдо-динамических подстановок, удовлетворяющих взаимоисключающим требованиями, в частности дифференциальным характеристикам, не уступающим фиксированным операциям подстановки той же размерности, является актуальной проблемой. Результатом является постановка общей научной задачи и формулировка частных задач диссертационных исследований.

Во второй главе содержится описание синтеза структуры псевдо-динамической операции подстановки на основе ARX-функций. Исследования демонстрируют, что объединение ARX-функций, имеющих откровенно слабые криптографические свойства, в структуру псевдо-динамической подстановки позволяет получать свойства эквивалентных подстановок, близкие к свойствам случайно сформированных подстановок аналогичной размерности. PD-sbox-ARX содержит простые операции и имеет заложенные возможности параллелизации обработки данных, что позволяет делать эффективные программные и аппаратные реализации для различных процессоров и аппаратных платформ.

Предложен метод синтеза псевдо-динамической функции PD-sbox-ARX-32, который позволяет получать PD-sbox-ARX с достаточно близкими к 8-раундовым преобразованиям Speck32 и miniAlzette32 криптографическими свойствами. При синтезе 100 PD-sbox-ARX 73 варианта имели вес разностных характеристик Wd равный 32 и вес линейных характеристик Wl, равный 13 и 14.

В третьей главе приведены результаты исследования дифференциальных и линейных характеристик PRF pCollapserARX, используя CASCADA. Проанализирован метод синтеза PD-sbox-ARX. Сделаны выводы о том, что подобранная структура 32-битной ARX-функции в составе PD-sbox 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.

Аналогичный результат получается при сравнении 32-битной ARX-функции с 8-итерационным 32-битным преобразованием из блочного криптоалгоритма Speck32. При аппаратной реализации ARX-функции данное свойство позволяет пропорционально уменьшить (до 4 раз) задержку при преобразовании блоков информации.

Предложенный метод синтеза параметров 32-битной ARX-функции позволяет 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. Сопоставимые

разностные и линейные характеристики имеют 8-итерационные 32-битная Alzette-подобная структура и 8-итерационное 32-битное преобразование из блочного криптоалгоритма Speck32.

Предложенный метод синтеза параметров 32-битной ARX-функции позволяет минимизировать количество затрачиваемых ассемблерных инструкций на операции циклического сдвига при реализации на малоресурсных 8-битных микроконтроллерах семейства AVR (например, ATmega328P).

В заключении формулируются выводы, основные результаты работы и рекомендации.

В приложениях приводятся акты о внедрении результатов диссертационной работы, а также свидетельство о государственной регистрации программы для ЭВМ.

Диссертация является завершённым научно-исследовательским трудом. Задачи, поставленные автором, решены полностью, цель исследования достигнута.

Основные положения диссертации опубликованы в 11 научных печатных работах, в том числе: 5 – в ведущих рецензируемых научных журналах, входящих в перечень ВАК РФ (из них 1 категории К1 и RSCI, 4 категории К2), 6 – в материалах конференций и других изданиях. Получено свидетельство о государственной регистрации программы для ЭВМ. Результаты работы прошли апробацию на научных конференциях различного уровня.

4. Соответствие специальности

Выполненное соискателем научное исследование соответствует паспорту специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность» по пункту 19 «Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов.».

5. Замечания по диссертационной работе

1. В работе не проанализированы потенциальные уязвимости PD-sbox-ARX-32 к иным криптографическим атакам, например, алгебраическим или атакам по сторонним каналам. Диссертантом не обоснован отказ от анализа таких криптографических атак для представленной подстановки.

2. Диссертант сравнивает разработанный PD-sbox-ARX только с алгоритмами Speck32 и Alzette. Диссертант не даёт глубокого сопоставления с иными актуальными стандартами.

3. Одно из выносимых на защиту Положений утверждает, что разработан универсальный метод синтеза PD-sbox-ARX, позволяющий путём подбора параметров ARX-функций минимизировать количество затрачиваемых ассемблерных инструкций на операции циклического сдвига при их реализации на малоресурсных 8-битных микроконтроллерах. Однако доказательство валидности метода синтеза приведено только для микроконтроллера ATmega328P.

4. При оценке разработанности темы диссертационного исследования проанализированы работы в основном криптографической школы ЮФУ. Следовало бы проанализировать и другие исследования псевдо-динамических операций подстановки PD-sbox.

6. Заключение

Диссертация Прудникова В. А. представляет собой законченную научно-квалификационную работу, посвящённую решению актуальной задачи, имеющей

важное значение в области информационной безопасности. Диссертация обладает научной новизной, имеет теоретическую значимость и практическую ценность. Полученные результаты в полной мере отражены в авторских публикациях. Автореферат полностью отражает содержание диссертации.

Диссертация отвечает требованиям, установленным Положением «О присуждении ученых 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.

Официальный оппонент
Доктор технических наук (05.12.04 «Радиотехника, в том числе системы и устройство телевидения»), профессор, заведующий кафедрой «Информационная безопасность» Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»,
Шелухин Олег Иванович

111024, г. Москва, ул. Авиамоторная, 8а, МТУСИ
Тел. служ.: +7 (495) 957-79-17, email: mtuci@mtuci.ru

«30» мая 2025 г. _____ О. И. Шелухин

Подпись О. И. Шелухина заверяю

Ученый секретарь
Ученого Совета МТУСИ Т.В. Зотова