ОТЗЫВ НАУЧНОГО РУКОВОДИТЕЛЯ

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»

Операции замены или фиксированные подстановки sbox являются основным нелинейным элементом для множества современных псевдослучайных функций PRF и псевдослучайных перестановок PRP, которые являются базовым элементом логической защиты информации в информационных системах.

Под термином «подстановка» (sbox, замена) в работе 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 PRF и PRP, 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), то от нелинейных свойств фиксированных подстановок напрямую зависит количество итераций, затрачиваемых вычислительных ресурсов, а также время обработки и потребляемая мощность.

Активно развиваются малоресурсные (легковесные) псевдослучайные функции и псевдослучайные перестановки, для которых в ущерб стойкости и времени обработки информации улучшаются показатели по затрачиваемым вычислительным ресурсам и потребляемой мощности. Их появление предопределено внедрением защищённых RFID меток, смарт-карт, устройств IoT и электронных устройств с ограниченными аппаратными ресурсами. На текущий момент представлено более 50 легковесных блочных криптоалгоритмов, десятки поточных криптоалгоритмов и хеш-функций. Часть из них является международными или национальными стандартами. Институт NIST США запустил конкурс по отбору и стандартизации легковесных псевдослучайных функций для малоресурсной электроники.

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.

Исследованию свойств и синтезу фиксированных подстановок научное сообщество посвятило более 40 лет (с момента появления первых блочных шифров). Научным коллективом авторов (Поликарпов С.В., Румянцев К.Е., Кожевников А.А., Петров Д.А.) предложен новый класс операций подстановки – псевдо-динамические подстановки (PD-sbox). Псевдо-динамические подстановки обладают как свойствами фиксированных подстановок (относительно низкие затраты вычислительных ресурсов), так и свойствами динамических подстановок (эффективное противодействие статистическим методам криптоанализа). Уникальные свойства псевдо-динамических подстановок требуют детальных исследований их криптографических характеристик.

Таким образом, сформулированная автором цель диссертационных

исследований – минимизация затрачиваемых ресурсов программной реализации криптографических преобразований при обеспечении заданных криптографических свойств, посредством разработки метода синтеза псевдо-динамических подстановок на основе ARX-функций, является актуальной научной задачей, состоящей в разработке и исследовании метода синтеза псевдо-динамических подстановок на основе ARX-функций, удовлетворяющих широкому спектру противоречивых требований по стойкости к криптоанализу и затрачиваемым ресурсам при программной реализации криптографических преобразований.

Диссертационные исследования соответствуют пункту 19 «Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов» паспорта научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность».

Проанализированы существующие подходы к синтезу и применению динамических и псевдо-динамических операций подстановки. Приведены выводы о том, что рассмотренные подходы 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 или иных фиксированных преобразований. В отличие от этого метод синтеза псевдо-динамических подстановок на основе ARX-функций, позволяет получать преобразования, удовлетворяющие требованиям по криптографическим свойствам, затрачиваемым ресурсам и скорости программной реализации криптографических преобразований.

Разработана структура 32-битной ARX-функции, позволяющая в составе PD-sbox обеспечить критический путь (максимальное количество последовательных операций сложения по модулю 2^{16}) в четыре раза меньше, чем ARX-преобразования, такие как 8-итерационная 32-битная Alzette-подобная структура, или 8-итерационное 32-битное преобразование криптоалгоритма Speck32, при двукратном увеличении количества операций и при сопоставимых максимальных значениях весов разностных и линейных характеристик.

Разработан 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 семейства AVR (например, ATmega328P) и, в отличие от метода случайного поиска оптимальных параметров, позволяет снизить количество соответствующих ассемблерных инструкций на 23,6% при программной реализации псевдо-динамической подстановки, включающей в свой состав четыре 32-битные ARX-функции.

Проанализирован разработанный метод синтеза псевдо-динамических подстановок на основе ARX-функций (PD-sbox-ARX). Сделаны выводы о том, что метод синтеза PD-sbox-ARX позволяет подобрать параметры для 32-битных ARX-функций, при которых, в отличие от 8-итерационного 32-битного преобразования криптоалгоритма Speck32, требуется на 10,6% меньше ассемблерных инструкций на операции циклического сдвига, при их реализации на малоресурсных 8-битных микроконтроллерах семейства AVR, и обеспечивается максимальный вес разностной характеристики равный 2^{-32} (эмпирический вес 2^{-26}) и вес линейной характеристики 2^{-13}.

Данные результаты относятся к п.19 паспорта специальности.

В качестве практической ценности автор выделил то, что применение псевдо-динамических подстановок на базе подобранных ARX-функций, обладающих дифференциальными и линейными свойствами эквивалентных подстановок, аналогичным 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. Данные результаты относятся к п.19 паспорта специальности.

К новым научным результатам диссертационной работы относятся:

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

– 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).

Результаты диссертационных исследований, посвящённых минимизации затрачиваемых ресурсов программной реализации криптографических преобразований при обеспечении заданных криптографических свойств, посредством разработки псевдо-динамических подстановок на основе ARX-функций, связаны с научным направлением кафедры информационной безопасности телекоммуникационных систем ЮФУ, что подтверждено соответствующим актом о внедрении результатов работы от 16.01.2024 г. Разработано и внедрено в учебный процесс программное обеспечение для анализа криптографических свойств (дифференциальные свойства, линейные свойства, алгебраический иммунитет, количество степеней свободы) псевдо-динамических операций подстановки на основе ARX-конструкций, акт внедрения ИКТИБ от 04.04.2024 г.

В целом, диссертационная работа Прудникова В. А. представляет собой целостное исследование, включающее постановку и решение актуальной научной задачи синтеза и исследования псевдо-динамических подстановок на основе ARX-функций, удовлетворяющих широкому спектру противоречивых требований по стойкости к криптоанализу и затрачиваемым ресурсам при программной реализации криптографических преобразований. Это свидетельствует о зрелости и самостоятельности диссертанта как научного работника.

Останавливаясь на характеристике общественной и научно-педагогической деятельности аспиранта, следует отметить, что Прудников В. А. за время работы над диссертационным исследованием проявил себя высококвалифицированным специалистом в области информационной безопасности, способным к самостоятельным исследованиям.

Считаю, что представленная работа удовлетворяет требованиям, установленным Положением «О присуждении учёных степеней в федеральном государственном автономном образовательном учреждении высшего образования «Южный федеральный университет», а её автор – Прудников Вадим Александрович заслуживает присуждения ему учёной степени кандидата технических наук по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность».

Научный руководитель, доктор технических наук, профессор Румянцев Константин Евгеньевич, зав. кафедрой «Информационная безопасность телекоммуникационных систем»

Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет»

Институт компьютерных технологий и информационной безопасности

Адрес: 347928, г. Таганрог, ул. Чехова, 2

Тел. 8 (8634) 68-08-90 IP 300-39

e-mail: rumyancev@sfedu.ru

Персональная страница: https://sfedu.ru/person/rumyancev

Специальность: 05.12.20 «Оптические системы локации, связи и обработки информации».

Я, Румянцев Константин Евгеньевич, даю согласие на включение моих персональных данных в документы, связанные с работой диссертационного совета и их дальнейшую обработку.

«4» декабря 2024 г. К. Е. Румянцев

Подпись заведующего кафедрой
информационной безопасности
телекоммуникационных систем заверяю.
Директор института компьютерных технологий
и информационной безопасности
Южного федерального университета

Г. Е. Веселов