На правах рукописи

ПРУДНИКОВ ВАДИМ АЛЕКСАНДРОВИЧ

СИНТЕЗ И ИССЛЕДОВАНИЕ ПСЕВДО-ДИНАМИЧЕСКИХ ПОДСТАНОВОК

Специальность 2.3.6 – «Методы и системы защиты информации, информационная безопасность»

АВТОРЕФЕРАТ
диссертации на соискание учёной степени
кандидата технических наук

Таганрог – 2025

Работа выполнена в ФГАОУ ВО «Южный федеральный университет» на кафедре информационной безопасности телекоммуникационных систем Института компьютерных технологий и информационной безопасности

Научный руководитель: **Румянцев Константин Евгеньевич**
доктор технических наук, профессор

Официальные оппоненты: **Шелухин Олег Иванович**
доктор технических наук, профессор,
ФГБОУ ВО «Московский технический университет связи и информатики»,
г. Москва, заведующий кафедрой «Информационная безопасность»

Панасенко Сергей Петрович
кандидат технических наук,
Акционерное общество «Актив-софт»,
г. Москва, директор по научной работе

Защита состоится «26» июня 2025 г. в 14:00 на заседании диссертационного совета ЮФУ801.02.02 Федерального государственного автономного образовательного учреждения высшего образования «Южный федеральный университет» по адресу: Ростовская обл., г. Таганрог, ул. Шевченко, 2, «Точка кипения» ИТА ЮФУ.

С диссертацией можно ознакомиться в Зональной научной библиотеке им. Ю.А. Жданова Южного федерального университета по адресу: г. Ростов-на-Дону, ул. Зорге, 21 Ж и на сайте: https://hub.sfedu.ru/diss/show/1338109.

Отзыв в 2-х экз. (*с указанием ФИО (полностью), ученой степени со специальностью, звания, организации, подразделения, должности, адреса, телефона, e-mail, даты*) с заверенной подписью рецензента и печатью учреждения просим направлять ученому секретарю диссертационного совета ЮФУ801.02.02 по адресу: 347922, Ростовская обл., г. Таганрог, пер. Некрасовский, 44, к. 302, а также в формате pdf – на e-mail: nbelchaninova@sfedu.ru.

Автореферат разослан « » мая 2025 г.

Учёный секретарь
диссертационного совета ЮФУ801.02.02,
кандидат технических наук, доцент Ельчанинова Н. Б.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы 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.

Степень разработанности темы. Существует множество подходов решения проблемы синтеза операций подстановки. Большинство заключается в применении различных методик при генерации фиксированных блоков замен, обладающих требуемыми криптографическими свойствами. Например, коллективом авторов – Ivanov G., Nikolov N., Nikova S. описан реверсивный

генетический алгоритм, использование которого позволяет быстро генерировать большое число стойких биективных подстановок размерностью от 8 до 16 бит, которые имеют неоптимальные свойства и сложную алгебраическую структуру, а также не обладают линейной избыточностью. Автором Tesař P. представлен метод генерации таблиц подстановок размерностью 8 бит с нелинейностью, достигающей значения 104. Метод комбинирует специальный генетический алгоритм с полным деревом поиска. Коллективом авторов – Kazymyrov O., Kazymyrova V., Oliynykov R. представлен метод генерации нелинейных sbox на основе градиентного спуска. Использование предложенного метода для наиболее часто применяемых подстановок, размерностью 8 бит, позволяет добиться показателей нелинейности 104.

Указанные подходы не удовлетворяют всем взаимоисключающим требованиям. В частности, размерность сгенерированной подстановки может не позволить эффективно применять её в программной или аппаратной реализации криптографических преобразований, в силу потребления большого объёма ресурсов.

Иной способ решения заключается в применении в качестве фиксированных подстановок ARX-функций. Например, авторами Bernstein D.J., Robshaw M., Billet O. представлено семейство поточных шифров Salsa20, основанное на ARX-операциях. Авторами Maitra S., Paul G., Meier W. представлены результаты криптоанализа Salsa20. Им удалось достичь сложности поиска ключа в $2^{247,2}$ при осуществлении анализа 8-раундовой реализации, что значительно превосходит результаты прошлых лет в 2^{251} и 2^{250}. Авторы Beaulieu R., Shors D., Smith J. разработали шифры Simon и Speck – легковесные блочные криптоалгоритмы, предназначенные для интернета вещей и построенные на основе ARX-функций. В статье «Cryptanalysis of the Speck Family of Block Ciphers» коллективом авторов – Abed F., List E., Lucks S., Wenzel J., представлены результаты дифференциального криптоанализа над описанными шифрами. Коллективом авторов (Beierle C., Micciancio D., Ristenpart T.) представлена 64-битная операция подстановки Alzette, основой которой являются ARX-функции. Особенностью преобразования является то, что оно вычисляется на современных процессорах за фиксированное время и использует всего 12 инструкций.

Недостатком подхода, подразумевающего использование ARX-операций, являются неудовлетворительные криптографические свойства создаваемых конструкций, однако они позволяют добиться высокого быстродействия и малого потребления ресурсов при программной и аппаратной реализации криптографических преобразований.

Для противодействия статистическим методам криптоанализа неоднократно осуществлялись попытки применять вместо фиксированных подстановок динамически изменяемые подстановки. Наиболее успешной попыткой применения динамически изменяемой подстановки можно назвать криптоалгоритм RC4, представленный автором Weerasinghe T. D. B. в работе «An Effective RC4 Stream Cipher», который считается устаревшим и

ненадёжным. Основная проблема стойкости RC4 – применение всего одной динамически изменяемой подстановки и медленное обновление содержимого подстановки (за одну итерацию обновляется 2 ячейки из 256), что опубликовано в статье Klein A. «Attacks on the RC4 stream cipher». Проблема предопределена тем, что динамические подстановки (в сравнении с фиксированными подстановками) требуют на порядки больше вычислительных ресурсов.

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). Применение псевдо-динамических операций подстановки на базе фиксированных замен потенциально позволяет решить ряд описанных выше проблем, в частности обеспечить устойчивость к статистическим методам криптоанализа. В свою очередь, применение подобранных ARX-функций для использования в структуре псевдо-динамических подстановок потенциально позволяет получить вес дифференциальных и линейных характеристик, превосходящий аналоги, при тех же затратах ресурсов при программной реализации криптографических преобразований.

В связи с вышесказанным возникает актуальная научная задача разработки и исследования 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.

Целью диссертационного исследования является минимизация затрачиваемых ресурсов программной реализации криптографических преобразований при обеспечении заданных криптографических свойств посредством разработки метода синтеза псевдо-динамических подстановок на основе ARX-функций.

Достижение поставленной цели предусматривает решение **частных задач:**

1. Анализ существующих подходов к синтезу псевдо-динамических операций подстановки.

2. Синтез структуры псевдо-динамической операции подстановки, удовлетворяющей широкому спектру противоречивых требований, посредством разработки метода синтеза псевдо-динамических подстановок на основе ARX-функций.

3. Анализ синтезированной псевдо-динамической функции PD-sbox-ARX-32 и её программной реализации на малоресурсных процессорах.

Объект исследования – криптографические операции подстановки, являющиеся составным элементом множества блочных шифров.

Предмет исследования – синтез и исследование псевдо-динамических операций подстановки, удовлетворяющих широкому спектру противоречивых требований по стойкости к разностному криптоанализу, а также затрачиваемым ресурсам при программной реализации криптографических преобразований.

Методы исследования: статистический криптоанализ с использованием SMT/SAT решателей, численные методы для оценки свойств псевдо-динамических подстановок, вычислительный эксперимент по определению криптографических свойств ARX-функций и псевдо-динамической функции PD-sbox-ARX-32.

Основные научные положения, выносимые на защиту:

1. 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 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.

2. Синтезированная 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 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.

3. Разработанный метод синтеза PD-sbox-ARX позволяет 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.

4. Разработанный метод синтеза псевдо-динамических подстановок на основе ARX-функций 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}.

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.

Достоверность результатов диссертационной работы подтверждается сходимостью исходной гипотезы с результатами опытно-экспериментальных данных, а также строгостью применяемого математического аппарата.

Внедрение результатов работы. Результаты диссертационного исследования, подтверждённые соответствующими актами, используются в:

– при подаче заявки «Метод синхронизации между абонентами локальной квантовой сети и доверенным узлом магистральной квантовой сети» на конкурс 2024 года Российского научного фонда «Проведение фундаментальных научных исследований и поисковых научных исследований малыми отдельными научными группами». В частности, формулирование частной научной задачи гранта, связанной с поиском возможных контрмер

против выявленных атак, основывается на научных результатах диссертационной работы в части метода синтеза псевдо-динамической подстановки PD-sbox-ARX-32 и структуры псевдо-динамической операции подстановки на основе ARX-функций;

– научной деятельности кафедры Информационной безопасности телекоммуникационных систем Института компьютерных технологий и информационной безопасности Южного федерального университета;

– учебном процессе кафедры Информационной безопасности телекоммуникационных систем Института компьютерных технологий и информационной безопасности Южного федерального университета, в части разработанной программы для ЭВМ.

Апробация результатов. Основные результаты работы докладывались и обсуждались на 5 научных конференциях:

– I Всероссийская научно-практическая конференция «Digital Era», г. Грозный, 26 марта 2021;

– VII Всероссийская научно-техническая конференция «Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности», г. Таганрог, 05-11 апреля 2021;

– VIII Всероссийская научно-техническая конференция «Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности», г. Таганрог, 04-09 апреля 2022;

– IX Всероссийская научно-техническая конференция «Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности», г. Таганрог, 10-15 апреля 2023;

– XII симпозиум «Современные тенденции в криптографии» (CTCrypt 2023) 6-9 июня 2023, г. Волгоград.

Публикации. 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.

Соответствие паспорту специальности. Диссертация соответствует 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».

Личный вклад автора. Основные научные результаты, в том числе структура псевдо-динамической операции подстановки на основе ARX-функций, метод синтеза параметров 32-битной ARX-функции, а также количественная оценка затрачиваемых ресурсов программной реализации разработанного криптографического преобразования и криптографических свойств получены автором лично.

Структура и объем диссертации. 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.

СОДЕРЖАНИЕ РАБОТЫ

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.

Для раскрытия возможностей ARX-функций в составе псевдо-динамических операций подстановки предложена ARX-конструкция, позволяющая эффективно использовать ресурсы и особенности процессоров и аппаратных платформ, в частности AVX-инструкции (Advanced Vector Extensions). Основными критериями синтеза ARX-функций являются использование сдвигов, кратных 8 бит, и параллельность выполнения представленных в ней операций, что способствует оптимальному использованию AVX-инструкций.

Выражение, описывающее 64-битную ARX-функцию (значения a и b являются 32-битными):

$$a_2 = \big((a_1 + (a_1 \ll t_0) \oplus b_1) \ll t_2\big) \oplus const_0, \quad (1)$$

$$b_2 = \big((b_1 + (b_1 \ll t_1) \oplus a_1) \ll t_3\big) \oplus const_1, \quad (2)$$

$$a_3 = (a_2 + \big((a_2 \ll t_4) \oplus b_2\big) \ll t_6), \quad (3)$$

$$b_3 = (b_2 + \big((b_2 \ll t_5) \oplus a_2\big) \ll t_7), \quad (4)$$

где $\oplus$ – сложение по модулю 2, $a \ll t$ – циклический сдвиг на t бит влево в двоичном слове a, a_1 – младшие 32 бит входного 64-битного значения, b_1 – старшие 32 бит входного 64-битного значения, a_3 и b_3 – младшие и старшие 32 бит выходного 64-битного значения, $t_0 \dots t_7$ – значения циклических сдвигов, задающие конкретную ARX-функцию, $const$ – 32-битные значения констант, задающие конкретную ARX-функцию.

Значения описанных параметров представлены в таблице 1.

Таблица 1 – Значения параметров ARX-функций

	t_0	t_1	t_2	t_3	t_4	t_5	t_6	t_7
funcARX0:	8	16	16	8	8	16	0	0
funcARX1:	8	16	8	16	16	8	8	8
funcARX2:	16	8	8	16	8	16	16	16
funcARX3:	16	8	16	8	16	8	24	24

Структура подобранной ARX-функции представлена на рисунке 1.

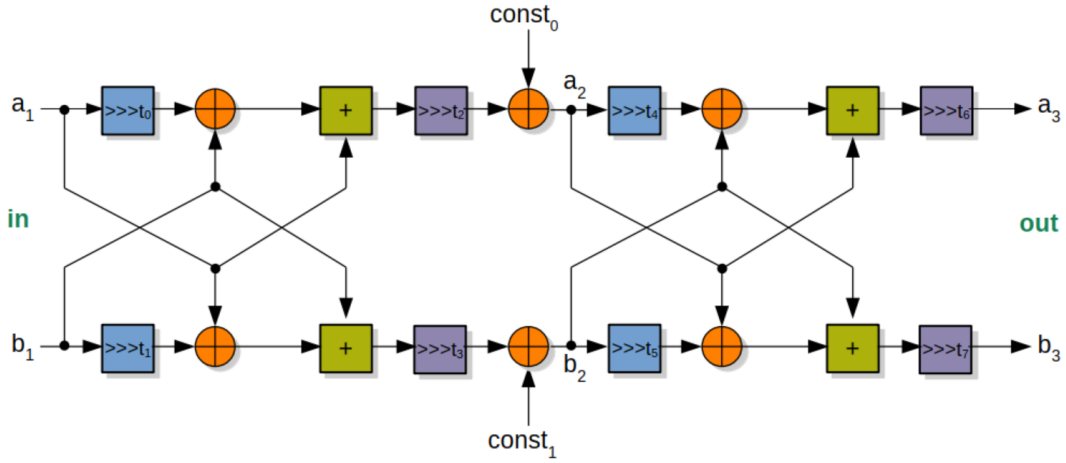

Рисунок 1 – Структура ARX-функции

На базе представленных ARX-конструкций построена 64-битная псевдо-динамическая операция подстановки PD-sbox_4x64x64, представленная на рисунке 2 и включающая 4 ARX-функции. Размер предполагаемого раундового ключа – 256 бит, размер управляющего состояния для изменения порождаемых операций подстановки – 256 бит. Суммарное значение внутреннего состояния – 512 бит.

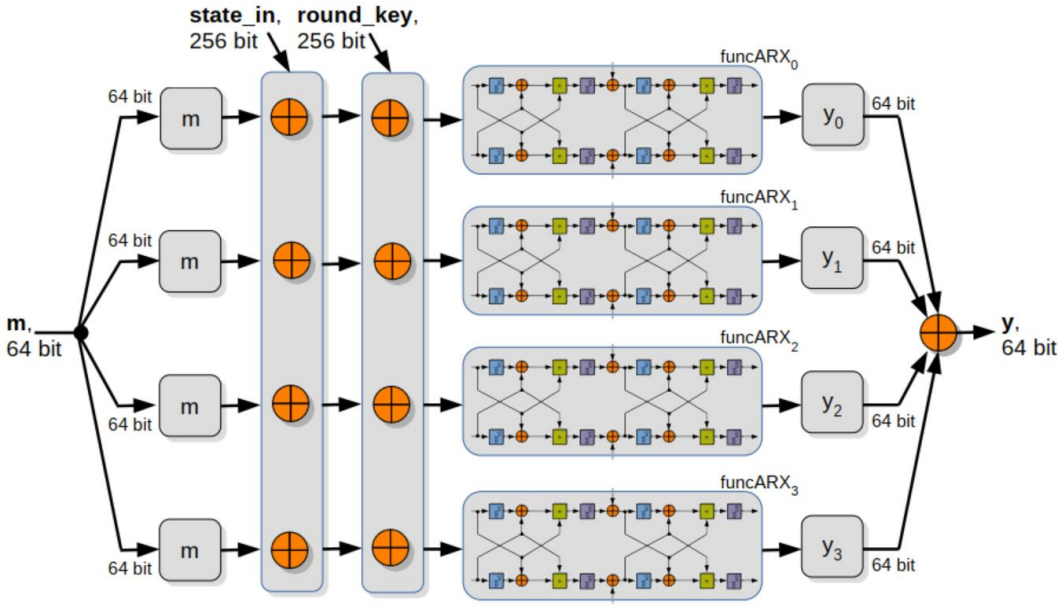

Рисунок 2 – PD-sbox_4x64x64

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 параллельной обработки данных, что позволяет обеспечить эффективные программные и аппаратные реализации для различных процессоров и аппаратных платформ.

Предложенный метод синтеза псевдо-динамической функции PD-sbox-ARX-32 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 имеют вес разностных характеристик Wd равный 32 и вес линейных характеристик Wl, равный 13 и 14.

Разработан универсальный метод синтеза PD-sbox-ARX, для микроконтроллеров семейства AVR. Доказательство эффективности предложенного метода приводится для микроконтроллера архитектуры AVR – ATmega328P и конкретной реализации псевдо-динамической функции PD-sbox-ARX-32. Метод синтеза заключается в следующем:

1. Эвристический выбор структуры ARX-функции с учётом возможных особенностей программной и аппаратной реализаций;

2. Начальное заполнение параметров циклических сдвигов ARX-функций (всего по 8 значений на 4 функции) значением 8;

3. Последовательный выбор каждого параметра ARX-функции, замена его на случайное значение из допустимого диапазона (от 0 до 15), проверка криптографических свойств (вес разностных и линейных характеристик) и ожидаемого количества затрачиваемых ассемблерных инструкций для

полученной версии ARX-функции. После обхода всех параметров первой ARX-функции выбирается наилучшая версия (при её наличии), которая заменяет исходную. Далее осуществляется переход к следующей ARX-функции для выполнения аналогичных действий;

4. Действия из пункта 3 повторяются до момента отсутствия улучшений в свойствах ARX-функций;

5. Формирование при помощи пунктов 2 и 3 набора наиболее удачных ARX-функций;

6. Выбор из набора наиболее удачных ARX-функций варианта с наименьшим количеством затрачиваемых ассемблерных инструкций для микроконтроллеров архитектуры AVR. В таблице 2.4 представлено количество ассемблерных инструкций для реализации 16-битовых операций ROL для 12 отобранных параметров PD-sbox-ARX-32.

Следует обратить внимание на следующее: по пункту 2 экспериментальные исследования показывают, что если сразу задать «удачный» вариант значений циклического сдвига (для 16-битных сдвигов значение равно 8), то значительно увеличивается вероятность того, что эти значения будут в результирующей ARX-функции после операций синтеза; по пункту 5 экспериментальные исследования показывают, что предложенный пошаговый подбор параметров 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 имеют вес разностных характеристик Wd равный 32 и вес линейных характеристик Wl, равный 13 и 14. Такие характеристики очень близки 8-раундовым преобразованиям Speck32 и miniAlzette32. Поэтому варианты с более худшими характеристиками исключаются из набора.

В результате получается 12 параметров, представленных в таблице 2. При этом наименьшее количество ассемблерных инструкций для архитектуры AVR составляет $N = 360$, что в 1,4 раза и 1,7 раза больше, чем для наихудшего и наилучшего вариантов синтеза соответственно, для которых $N = 256$ и $N = 217$.

Таблица 2 – Количество ассемблерных инструкций для реализации 16-битовых операций ROL для 12 отобранных параметров PD-sbox-ARX-32

№	**Архитектура микроконтроллера**		
	AVR	mips64	ARM
1	242	150	73
2	248		
3	256		
4	222		
5	242		
6	248		

Продолжение таблицы 2

№	Архитектура микроконтроллера		
	AVR	mips64	AVR
7	240	150	73
8	231		
9	**217**		
10	234		
11	234		
12	248		

В таблице 3 приведено сравнение свойств лучшей синтезированной PD-sbox-ARX-32 со свойствами 8-итерационной 32-битной Alzette-подобной структуры и 8-итерационным 32-битным преобразованием из блочного криптоалгоритма Speck32.

Таблица 3 – Количество ассемблерных инструкций для реализации 16-битовой операций ROL

Преобразование	Архитектура микроконтроллера			Криптографические свойства			
	AVR	mips64	ARM	Wd	Wde	Wl	Wle
miniAlzette32 (8 раундов)	154	70	42	27	~27	13	~13
Speck32 (8 раундов)	240	80	48	24	~24	12	~12
PD-sbox-ARX-32	**217**	**150**	**73**	**32**	**~26**	**13**	**~13**

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.

В силу размерности и сложности анализируемых конструкций, для поиска разностных и линейных свойств использован метод поиска криптографических характеристик, использующий SAT-решатели, в частности – фреймворк CASCADA. Создатели данного фреймворка особое внимание уделили анализу ARX-функций. В настоящее время SAT-решатели

являются одним из основных методов поиска и валидации криптографических свойств и характеристик криптографических преобразований.

PD-sbox-ARX-32 является невзаимнооднозначной псевдо-динамической функцией, несмотря на это, её анализ с использованием SAT/SMT-решателей возможен и найденные характеристики будут валидны. В качестве примера следует привести работу «Logical cryptanalysis as a SAT-problem: Encoding and analysis» за авторством – Massacci F., Marraro L., в которой представлены результаты первого криптоанализа шифра DES с использованием SAT-решателей.

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

Реализация криптографических преобразований на микроконтроллерах (малоресурсных процессорах) является важнейшей задачей, обусловленной как повсеместным использованием криптографических преобразований в сетевых протоколах, так и значительной ресурсоёмкости этих преобразований, что может привести к дефициту вычислительных ресурсов для основных процессов.

Стоит отметить, что на различных процессорах/микроконтроллерах для ARX-операций может требоваться разное количество тактов на их выполнение. Однако, для относительно простых микроконтроллеров предполагается, что на выполнение операций ADD или XOR требуется один такт. Однако, выполнение операции ROL может требовать значительного количества инструкций и тактов микроконтроллера.

В качестве таких процессоров/микроконтроллеров рассмотрены широко распространённые 8-битные микроконтроллеры AVR фирмы Atmel, микроконтроллеры ATmega328P (применяется, например, в Arduino UNO R3) и микроконтроллеры на базе инструкций MIPS32/MIPS64 (самым известным является семейство микроконтроллеров PIC32 от Microchip).

Для определения количества инструкций на операции циклического сдвига с разным количеством сдвигаемых бит воспользовались ресурсом godbolt.org, позволяющим в интерактивном режиме, как вывести результат компиляции исходного кода в виде набора ассемблерных инструкций, так и

легко выбрать компилятор и архитектуру/семейство целевого процессора или микроконтроллера.

Применён типовой способ описания операции ROL на языке C в виде типовой конструкции из двух нециклических сдвигов (влево и вправо) и объединения результатов при помощи операции OR или XOR. Для каждого значения циклического сдвига реализована отдельная функция, что позволило оценить количество затрачиваемых инструкций для ROL с разным значением сдвига.

После компиляции для каждой функции подсчитано количество требуемых на реализацию ассемблерных инструкций. При этом инструкция RET (возврат из функции) не учитывается, так как при компиляции целиком всей ARX-функции обычно осуществляется встраивание кода ROL-функции непосредственно в точку вызова функции (вместо её фактического вызова, что позволяет снизить количество инструкций вызова и возврата).

В таблице 4 приведены сводные значения по количеству инструкций на реализацию операции 16-битового циклического сдвига для рассматриваемых архитектур.

Таблица 4 – Количество ассемблерных инструкций для реализации 16-битовой операций ROL в зависимости от значения циклического сдвига

Операция	**Количество инструкций для архитектуры/компилятора**				
	AVR (gcc 14.1.0)	Arduino Uno (1.8.9)	mips32/64 (gcc 14.1.0)	ARM (gcc 14.1.0)	x86-64 (gcc 14.2)
ROL-1	**3**	**3**	5	3	2
ROL-2	17	18			
ROL-3	17	18			
ROL-4	13	14			
ROL-5	17	18			
ROL-6	17	18			
ROL-7	13	14			
ROL-8	**3**	**3**			
ROL-9	13	14			
ROL-10	17	18			
ROL-11	17	18			
ROL-12	13	14			
ROL-13	17	18			
ROL-14	17	18			
ROL-15	**4**	**4**			

Следует обратить внимание на то, что иные операции (сложение по модулю, XOR) соответствуют одной ассемблерной инструкции и ими можно пренебречь.

Для оценки эффективности предложенного метода сформировано 100 000 случайных наборов параметров ARX-функций для PD-sbox-ARX-32, для которых определено количество затрачиваемых ассемблерных

инструкций и криптографические свойства – вес разностных характеристик Wd, вес линейных характеристик Wl. Данный универсальный метод применён для сравнения, так как иные методы синтеза параметров PD-sbox-ARX не представлены в открытой печати.

Результаты в виде гистограмм распределения по количеству затрачиваемых ассемблерных инструкций приведены на рисунке 3, в виде гистограмм распределения по весам разностных Wd и линейных Wl характеристик – на рисунке 4.

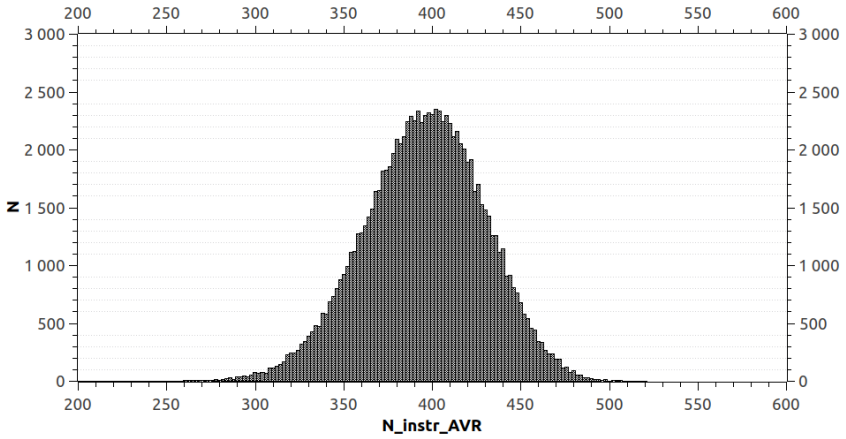

Рисунок 3 – Гистограмма распределения наборов параметров по количеству затрачиваемых ассемблерных инструкций

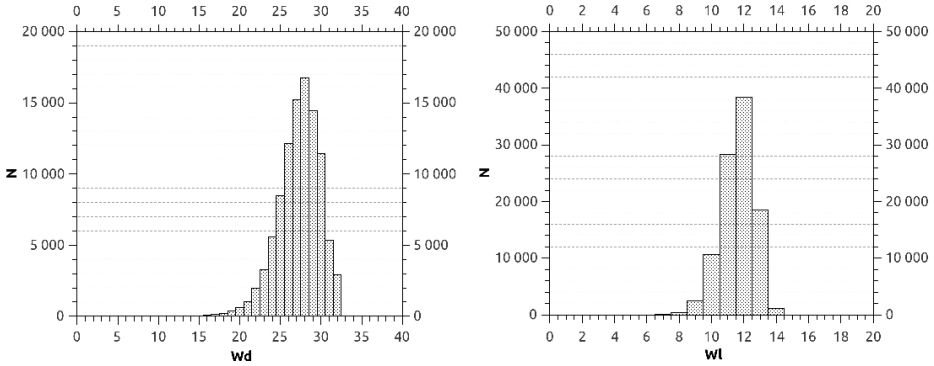

Рисунок 4 – Гистограмма распределения по весам разностных Wd и линейных Wl характеристик

Анализ гистограммы на рисунке 3, позволяет выделить 5 комбинаций параметров, выделенных на рисунке 5, обладающих минимальным количеством затрачиваемых ресурсов. Свойства параметров приведены в таблице 5.

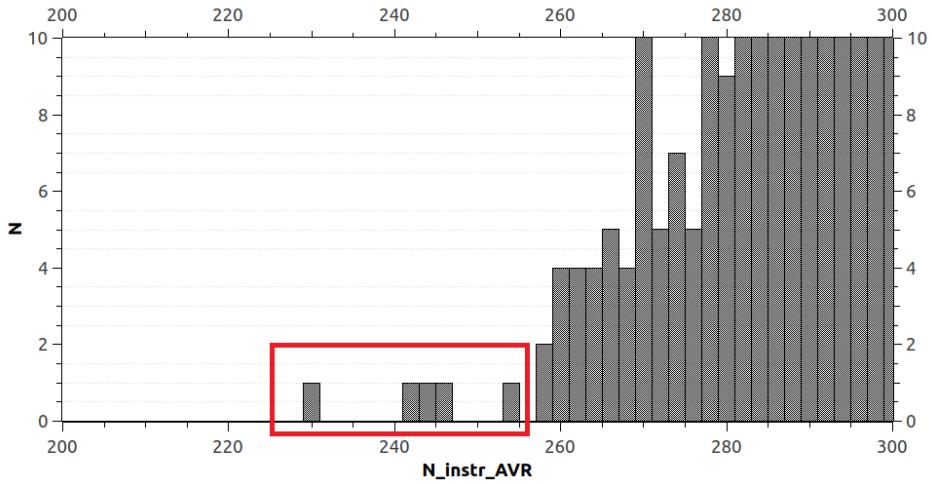

Рисунок 5– Параметры, обладающие минимальным количеством затрачиваемых ресурсов при использовании метода случайного подбора

Таблица 5 – Свойства 5 случайно подобранных комбинаций параметров

N	**AVR**	$\boldsymbol{Wd}$	$\boldsymbol{Wl}$
1	230	24	9
2	243	20	10
3	244	18	8
4	245	20	11
5	246	25	12
Синтезированный PD-sbox-ARX	**217**	**32**	**13**

Все случайно подобранные комбинации параметров ARX-функций с минимальным количеством затрачиваемых ассемблерных инструкций обладают неприемлемыми криптографическими характеристиками. Однако, даже в данном случае они существенно уступают синтезированному PD-sbox-ARX по количеству затрачиваемых ресурсов. При сравнении с вариантом 1 из таблицы 5, разница составляет ~5%, учитывая его неудовлетворительные криптографические характеристики.

На рисунке 6 приведены результаты в виде гистограмм распределения по количеству затрачиваемых ассемблерных инструкций, минимальное значение затрачиваемых ассемблерных инструкций равно 284 при $Wd > 29$ и $Wl > 10$.

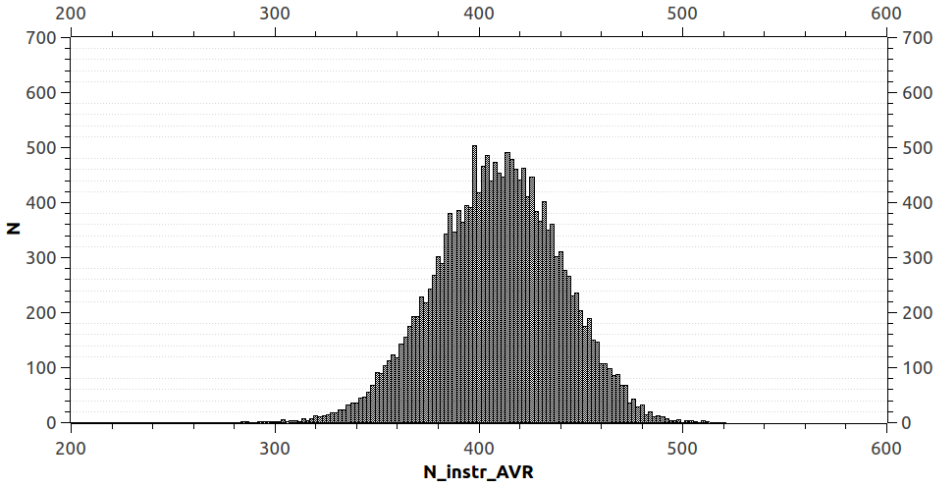

Рисунок 6 – Распределение наборов параметров по количеству затрачиваемых ассемблерных инструкций при $Wd > 29$ и $Wl > 10$

Анализ гистограммы на рисунке 6, позволяет выделить 5 комбинаций параметров, выделенных на рисунке 7, обладающих минимальным количеством затрачиваемых ресурсов при $Wd > 29$ и $Wl > 10$. Свойства параметров приведены в таблице 6.

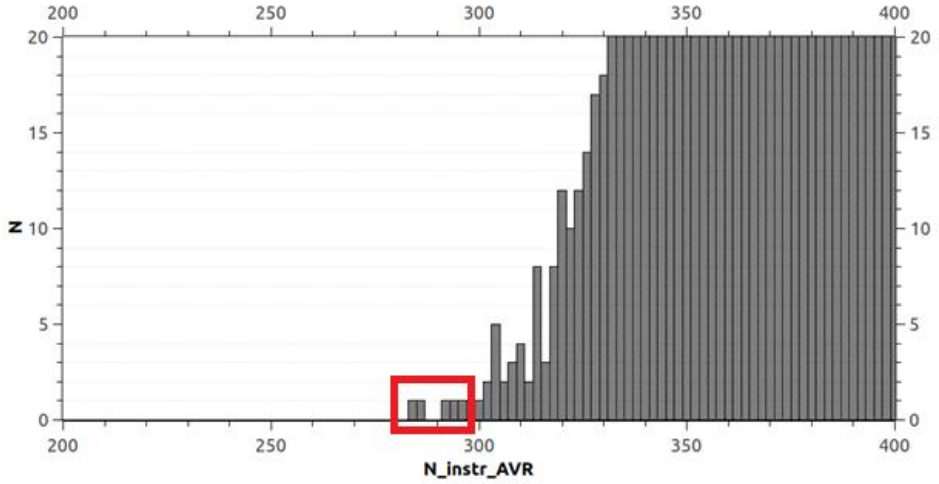

Рисунок 7 – Параметры, с минимальным количеством затрачиваемых ресурсов, метод случайного подбора при $Wd > 29$ и $Wl > 10$

Таблица 6 – Свойства 5 случайно подобранных комбинаций параметров при $Wd > 29$ и $Wl > 10$

N	**AVR**	$\boldsymbol{Wd}$	$\boldsymbol{Wl}$
1	284	30	11
2	286	30	11
3	292	30	11
4	294	31	11
5	297	30	11
Синтезированный PD-sbox-ARX	**217**	**32**	**13**

Все случайно подобранные комбинации параметров ARX-функций с минимальным количеством затрачиваемых ассемблерных инструкций обладают удовлетворимыми криптографическими свойствами, однако существенно уступают синтезированному PD-sbox-ARX по количеству затрачиваемых ресурсов. При сравнении с вариантом 1 из таблицы 6, разница составляет ~24%, без учёта уступающих криптографических свойств.

В свою очередь, применение разработанного метода для ранее рассмотренных криптографических преобразований – Speck32 и miniAlzette32 демонстрирует его универсальность.

Для проверки эффективности подбора параметров miniAlzette32 использовались 4 попытки (по 100 итераций подбора параметров в каждой попытке) и 8 итераций преобразования miniAlzette32. В таком случае, исходное значение параметров (значений циклических сдвигов) miniAlzette32 представляется в виде [15,12,9,9,0,15,12,8, 15,12,9,9,0,15,12,8,], а количество ассемблерных инструкций на исходную реализацию циклических сдвигов для микроконтроллеров архитектуры AVR составляет 126. Результаты поиска наилучших параметров для miniAlzette32 приведены в таблице 7. В одной из попыток удалось уменьшить количество затрачиваемых ресурсов на 31,7 % (со 126 до 86) для архитектуры AVR при сопоставимых значениях $Wd \geq 27$ и $Wl \geq 13$.

Необходимо отметить, что при синтезе подстановок учитываются криптографические свойства как самого sbox, так и результирующего преобразования, в котором подстановки разных итераций связаны через перемешивающие операции. Для Alzette приведены, в качестве основных, линейные и разностные свойства. При этом в разработанный метод можно добавить как учёт иных криптографических свойств, так и оценку свойств результирующих преобразований. Ограничением будут выступать возможности SAT-решателя и вычислительной техники по определению криптографических свойств за приемлемое время.

Таблица 7 – Параметры miniAlzette32 при применении разработанного метода синтеза параметров PD-sbox-ARX, при $Wd \geq 27$ и $Wl \geq 13$

ROT	**AVR**	**Улучшение, %**
[15, 12, 9, 9, 0, 15, 12, 8] оригинальные параметры	126	–
[15, 12, 9, 9, 0, 1, 12, 8] синтезированные параметры	124	1,6
[1, 12, 15, 9, 0, 1, 12, 8] синтезированные параметры	104	17,4
[15, 12, 1, 1, 0, 15, 12, 8] синтезированные параметры	**86**	**31,7**

Для проверки эффективности подбора параметров Speck32 использовались 4 попытки (по 100 итераций подбора параметров в каждой попытке) и 8 итераций преобразования Speck32. В таком случае, исходное

значение параметров (значений циклических сдвигов) Speck32 представляется в виде [7,2,7,2,7,2,7,2, 7,2,7,2,7,2,7,2] и количество ассемблерных инструкций на исходную реализацию циклических сдвигов для микроконтроллеров архитектуры AVR составляет 240. Результаты поиска наилучших параметров для Speck32 приведены в таблице 8. Помимо улучшения значений $Wd \geq 24$ и $Wl \geq 11$ в одной из попыток удалось уменьшить количество затрачиваемых ресурсов на 37,5 % (с 240 до 150) для архитектуры AVR.

Таблица 8 – Параметры Speck32 при применении разработанного метода синтеза параметров PD-sbox-ARX, при $Wd \geq 24$ и $Wl \geq 11$

ROT	**AVR**	**Улучшение, %**
[7,2,7,2,7,2,7,2] оригинальные параметры	240	–
[7, 9, 8, 2, 15, 4, 12, 2] синтезированные параметры	186	22,5
[7, 2, 7, 4, 7, 8, 1, 3] синтезированные параметры	184	23,3
[15, 3, 15, 12, 7, 14, 15, 8] синтезированные параметры	**150**	**37,5**

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.

ЗАКЛЮЧЕНИЕ

В результате диссертационного исследования решена актуальная научная задача и достигнута поставленная цель, заключающаяся в минимизации затрачиваемых ресурсов программной реализации криптографических преобразований при обеспечении заданных криптографических свойств посредством разработки метода синтеза псевдо-динамических подстановок на основе ARX-функций. Это подтверждается следующими полученными научными и практическими результатами:

1. Предложенный 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.

2. 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.

3. 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 архитектуры AVR. Доказательство эффективности предложенного метода приведено для микроконтроллера архитектуры AVR – ATmega328P и конкретной реализации псевдо-динамической функции PD-sbox-ARX-32. В отличие от метода случайного поиска оптимальных параметров, разработанный метод позволяет снизить количество соответствующих ассемблерных инструкций на 23,6% при программной реализации псевдо-динамической подстановки, включающей в свой состав четыре 32-битные ARX-функции.

4. Метод синтеза псевдо-динамических подстановок на основе ARX-функций (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, в частности ATmega328P, и обеспечивается максимальный вес разностной характеристики, равный 2^{-32} (эмпирический вес 2^{-26}), и вес линейной характеристики 2^{-13}.

СПИСОК ПУБЛИКАЦИЙ

Статьи в научных изданиях, входящих в Перечень ВАК

1. Прудников, В. А. Анализ существующих подходов к синтезу псевдо-динамических sbox / В. А. Прудников // Вопросы кибербезопасности. – 2024. – № 4(62). – С. 57-64. – DOI 10.21681/2311-3456-2024-4-57-64. (К1, RSCI).

2. Поликарпов, С. В. Синтез псевдо-динамических функций PD-sbox-ARX-32 / С. В. Поликарпов, В. А. Прудников, К. Е. Румянцев // Известия ЮФУ. Технические науки. – 2024. – № 5(241). – С. 102-118. – DOI 10.18522/2311-3103-2024-5-102-118. (К2).

3. Поликарпов, С. В. Исследование свойств миниверсии псевдо-случайной функции pCollapser / С. В. Поликарпов, В. А. Прудников, К. Е. Румянцев // Известия ЮФУ. Технические науки. – 2022. – № 6(230). – С. 148-162. – DOI 10.18522/2311-3103-2022-6-148-162. (К2).

4. Поликарпов, С. В. Вычислительно эффективный метод определения усреднённых линейных свойств псевдо-динамических подстановок / С. В. Поликарпов, В. А. Прудников, К. Е. Румянцев // Известия ЮФУ. Технические науки. – 2020. – № 5(215). – С. 16-30. – DOI 10.18522/2311-3103-2020-5-16-30. (К2).

5. Псевдослучайная функция pCollapser, обеспечивающая экстремальный параллелизм обработки информации / С. В. Поликарпов, В. А.

Прудников, А. А. Кожевников, К. Е. Румянцев // Известия ЮФУ. Технические науки. – 2019. – № 5(207). – С. 88-100. – DOI 10.23683/2311-3103-2019-5-88-100. (К2).

Публикации в сборниках трудов конференций

6. Прудников, В. А. Исследование нелинейных свойств псевдодинамической подстановки Pd-sbox 6x4x4 / В. А. Прудников // V Всероссийская научно-техническая конференция молодых ученых, аспирантов, магистрантов и студентов «Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности» : сборник статей Всероссийской научно-технической конференции, 01-07 апреля 2019 г. / Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет». – Таганрог, 2019. – С. 96-99. – Режим доступа: https://ictis.sfedu.ru/wp-content/uploads/2019/05/Sbornik-V.pdf (дата обращения 03.04.2025).

7. Прудников, В. А. Анализ линейных свойств псевдо-динамической подстановки на базе ARX-конструкций / В. А. Прудников // Неделя науки 2022 : сборник тезисов : в двух частях. Ч. 1 / Министерство науки и высшего образования Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет» ; редакционная коллегия: Я. А. Асланов [и др.]. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2022. – С. 619-623.

8. Прудников, В. А. Программный инструмент анализа нелинейных характеристик криптографических подстановок, использующий многопоточные вычисления / В. А. Прудников // Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности : VII Всероссийская научно-техническая конференция : сборник статей Всероссийской научно-технической конференции, 5-11 апреля 2021 / Министерство науки и высшего образования Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего образования "Южный федеральный университет". – Таганрог, 2021. – С. 123-125. – Режим доступа: https://clck.ru/3KTgBM (дата обращения 03.04.2025).

9. Прудников, В. А. Исследование распределения нелинейных свойств эквивалентных подстановок для псевдодинамических подстановок Pd-sbox-2x8 / В. А. Прудников // VI Всероссийская научно-техническая конференция молодых ученых, аспирантов, магистрантов и студентов «Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности» : сборник статей Всероссийской научно-технической конференции, 06-12 апреля 2020 г. / Министерство науки и высшего образования Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего образования "Южный федеральный университет". – Таганрог, 2020. – С. 123-127. – Режим доступа:

https://ictis.sfedu.ru/wp-content/uploads/2020/06/2020_proceedings.pdf (дата обращения 03.04.2025).

10. Поликарпов, С. В. Программные инструменты анализа нелинейных свойств криптографических подстановок / С. В. Поликарпов, В. А. Прудников, К. Е. Румянцев // I Всероссийская научно-практическая конференция «Digital Era», 26.03.2021 / Министерство науки и высшего образования Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего образования «Чеченский государственный университет», Факультет информационных технологий ; ответственный редактор: Хасухаджиев А.С.-А. – Грозный, 2021. – С. 138-141. – DOI 10.36684/38-2021-1-138-141.

11. Прудников, В. А. Анализ количества активных ARX-функций для мини-версии PRF pCollapser-ARX / В. А. Прудников // Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности : сборник статей IX Всероссийской научно-технической конференции Таганрог, 10–15 апреля 2023 г. / Министерство науки и высшего образования Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего образования "Южный федеральный университет". – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2023. – С. 61-64. – Режим доступа: https://ictis.sfedu.ru/wp-content/uploads/2023/05/IX_%D0%9A%D0%BE%D0%BD%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D0%B8%D1%8F.pdf (дата обращения 03.04.2025).

Свидетельства о государственной регистрации программ для ЭВМ

12. Свидетельство о государственной регистрации программы для ЭВМ № 2024610931 Российская Федерация. Программа анализа криптографических свойств псевдо-динамических операций подстановки на основе ARX-конструкций : № 2023688912 : заявл. 21.12.2023 : опубл. 16.01.2024 / С. В. Поликарпов, В. А. Прудников, К. Е. Румянцев ; правообладатель федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет».

Личный вклад автора в работы, выполненные в соавторстве:

В [2] разработан метод синтеза параметров 32-битной ARX-функции, получена количественная оценка затрачиваемых ресурсов программной реализации разработанного криптографического преобразования и криптографических свойств. В [3] доказано, что использование псевдо-динамических подстановок на основе ARX-функций в PRF семейства pCollapser позволяет получить из набора 4 ARX-функций с предельно низкими криптографическими свойствами, качественную нелинейную функцию, что подтверждает правильность концепции псевдо-динамических подстановок PD-sbox. В [4] разработан вычислительно эффективный метод определения усреднённых линейных свойств псевдо-динамических подстановок для K-элементных PD-sbox. В [5] разработана псевдо-случайная функция на основе

PD-sbox – "pCollapser". В [10] исследованы программные инструменты анализа криптографических свойств sbox. В [12] разработан алгоритм работы программы.