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 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 – от substitution box, таблица замен) подразумевается как взаимно однозначное, так и не взаимно однозначное преобразование m-битного значения на входе в n-битное значение 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 ряд 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 (Galois/Counter Mode – GCM) и схожих с ним режимах, в ряде 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 результирующей 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, формулируется 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, рассматривается 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 требованиям, 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 с использованием инструментария 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}, и вес линейной характеристики 2^{-13} для результирующей PD-sbox-ARX, включающей в свой состав четыре 32-битные ARX-функции. Сопоставимые разностные и линейные характеристики имеют 8-итерационная 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) Можно отметить некоторую небрежность автора диссертационной работы в части используемой терминологии, в частности:

- во введении англоязычный термин Authenticated Encryption with Associated Data – AEAD (аутентифицированное шифрование с присоединёнными данными) ошибочно определён как «Псевдослучайные функции, работающие в режиме счётчика с аутентификацией Галуа», хотя данный режим является только частным случаем AEAD-режимов и ему соответствует другой англоязычный термин Galois/Counter Mode – GCM;

- в разделе 1.4 разность между двоичными строками раскрыта только как результат операции «исключающее или» между строками; не указано, что такое определение является частным;

- в подразделе 3.1.6 применены термины relatedkey differential, impossible-differential, related-key impossible-differential и zerocorrelation cryptanalysis, вместо которых следовало применить соответствующие русскоязычные термины; кроме того, данные термины не определены.

2) В разделе 1.5 даётся подробное описание инструментария CASCADA; приведённое описание обладает значительной избыточностью для целей диссертационной работы.

3) Недостаточно подробно рассмотрены вопросы ресурсоёмкости аппаратной реализации подстановок PD-sbox-ARX при высокой актуальности применения аппаратных реализаций симметричных криптографических алгоритмов в устройствах с ограниченными ресурсами.

4) В подразделе 3.1.6 упоминаются криптографические алгоритмы SKINNY, NOEKEON и RECTANGLE без указания в диссертационной работе литературных источников, в которых данные алгоритмы определены.

Приведённые замечания не являются значительными по сравнению с отмеченными выше теоретической значимостью и практической ценностью данной диссертационной работы.

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:
кандидат технических наук
(05.13.01 «Системный анализ,
управление и обработка информации»),
директор по научной работе
Акционерного общества «Актив-софт»
Панасенко Сергей Петрович /С. П. Панасенко/

115088, г. Москва, ул. Шарикоподшипниковская, дом 1, помещение IX, комната 11.
Тел. служ.: +7 (495) 925-77-90, email: panasenko@guardant.ru

Подпись Панасенко С. П. заверяю

Генеральный директор
Акционерного общества «Актив-софт» /К. А. Черников/

Акционерное общество «Актив-софт» г. Москва
М.П.