Отзыв

официального оппонента

доктора технических наук, профессора **Молдовяна Николая Андреевича**

на диссертацию **Тихонова Сергея Владимировича**

на тему «**Исследование и разработка модификаций аппаратно-реализованных защитных блоковых преобразований, устойчивых к побочным атакам по цепям электропитания**», представленной на соискание ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Актуальность темы диссертационной работы

Диссертация Тихонова С.В. посвящена исследованию как теоретических, так и практических аспектов реализации атак с использованием побочных каналов по цепям электропитания (побочных атак), а также разработке метода защиты от атак данного типа. На сегодняшний день широкое распространение, в том, числе и в нашей стране, получили микрочипы, выполняющие процедуры идентификации и аутентификации, которые используются, например, в электронных идентификационных документах, проездных, смарт-картах. Такие чипы выступают в качестве защищенной от вскрытия среды, в которой выполняются некоторые защитные преобразования с целью аутентификации пользователей или данных. Практическая невозможность подделки (клонирования) подобных чипов, связывается со стойкостью выполняемых ими защитных преобразований к множеству известных атак. Применение апробированных стойких защитных преобразований обеспечивает несомненную стойкость к известным типам криптографических атак, однако для указанных приложений могут быть реализованы атаки с использованием утечки дополнительной информации по цепям электропитания чипа. Такие атаки позволяют извлечь секретные данные хранящиеся в чипе, в том числе ключ, реализованного на нём алгоритма защитного преобразования, за вполне

обозримое время. Эффективные способы защиты от побочных атак предложены для ряда широко используемых зарубежных алгоритмов защитных преобразований, в частности для блочных шифров DES и AES. Однако до сегодняшнего дня эффективных способов защиты блочных шифров, описанных российским стандартом ГОСТ Р 34.12-2015, не было опубликовано.

На текущий момент времени анализ стойкости реализаций алгоритмов защитных преобразований в микрочипах к атакам с использованием побочных каналов, в том числе к побочным атакам по цепи электропитания чипа, остается весьма актуальной задачей в целом и чрезвычайно актуальной задачей по отношению к защитным преобразованиям по стандарту ГОСТ Р 34.12-2015. Также чрезвычайно актуальной является задача разработки методов защиты аппаратных реализаций блочных шифров ГОСТ Р 34.12-2015 от атак по побочным каналам.

Таким образом, задача исследования побочных атак по цепям электропитания и разработки метода защиты от них является весьма актуальной для обеспечения информационной безопасности, в том числе и отечественных разработок.

Цель диссертационной работы Тихонова С.В. состояла в повышении информационной безопасности информационно-телекоммуникационных технологий в части безопасной аппаратной реализации защитных преобразований. Для её достижения автор в начале систематизировал и подробно описал известные на сегодняшний день знания о различных аспектах реализации атак по цепям электропитания, и в частности наиболее известной из них – разностном анализе мощности (DPA). Он впервые подробно описал особенности зависимостей энергопотребления взятого им тестового чипа от обрабатываемых данных. При этом измерения производились на специально разработанной им для этого установке. Автор составил достаточно подробную модель энергопотребления чипа, проработав таким образом ряд практических аспектов реализации атаки. Далее им были составлены модели атаки DPA применительно к российским блочным шифрам, описанным в стандарте

ГОСТ Р 34.12-2015, и осуществлён сравнительный анализ эффективности реализации атаки данного типа на эти шифры, а затем разработанная измерительная установка применена для выполнения натурного эксперимента, предполагающего взлом шифра «Магма», реализованного на реальном чипе. Результаты показали применимость общего подхода к реализации атаки DPA на блочные шифры, используемые за рубежом (AES, DES, 3DES и др.), и ГОСТ Р 34.12-2015 включая возможность восстановления ключа незащищённой аппаратной реализации российского шифра за несколько часов. Затем, основываясь на анализе известных знаний об атаке DPA и методов защиты от неё, а также на результатах проведённых аналитических и экспериментальных исследований автор предложил новый метод защиты блочных защитных преобразований от DPA. Предложенный метод отличает оригинальная идея, состоящая в том, что вместо внесения изменений в операции, составляющие алгоритм защитного преобразования, предлагается производить два дополнительных достаточно простых и защищенных от DPA преобразования с встроенным ключом: перед выполнением алгоритма (предобработка) и после него (постобработка). Этим достигается универсальность метода защиты (возможность его использования для обеспечения защиты любых преобразований, выполняемых чипом) и относительно низкие требования к дополнительным аппаратным ресурсам чипа. При этом защищённость от DPA определяется вычислительной сложностью перебора дополнительного ключа.

Научная новизна положений и результатов диссертационной работы

К новым научным результатам, полученным в диссертации, на мой взгляд можно отнести следующее:

1) Дополнена модель атаки по цепям электропитания экспериментальными результатами анализа зависимостей энергопотребления интегрального чипа от обрабатываемых им данных.

2) Представлены модели атаки DPA для аппаратных реализаций российских блочных шифров ГОСТ, произведено сравнение эффективности реализации к ним атаки DPA и проведён натурный эксперимент взлома российского шифра. Была показана уязвимость российских шифров относительно побочных атак по цепям электропитания.
3) Разработан новый метод защиты выполняемых чипом преобразований, от атак по цепям электропитания. Описанный метод является универсальным, подходит для защиты любых блочных защитных преобразований, в том числе и российских шифров ГОСТ. При этом обеспечивается сравнительно низкая стоимость реализации и относительно небольшие требования к дополнительным аппаратным ресурсам чипа. Скорость выполнения алгоритма шифра, защищённого таким методом, снижается меньше, чем в случае применения известных аналогов (методов маскировки и балансировки) применительно к зарубежным шифрам (типа DES, AES).

Достоверность и обоснованность основных полученных результатов

Достоверность и обоснованность полученных в диссертационном исследовании результатов обеспечивается анализом текущего состояния исследований в этой области, корректным использованием математического аппарата, результатами компьютерного моделирования и проведённых экспериментальных исследований. Подтверждением достоверности результатов исследования также служит обсуждение и одобрение их на научных конференциях и семинарах, а также положительные итоги практического использования в АО «Научные приборы», подтвержденные, приложенным к диссертации актом о внедрении результатов диссертации, на данном предприятии.

Теоретическая и практическая значимость

Теоретическая значимость полученных результатов связана с расширением класса методов безопасной аппаратной реализации защитных преобразований и предложенной автором архитектурой измерительной установки, позволяющей построить новые типы аппаратуры для выполнения атаки DPA, использование которой значительно удешевляет стоимость реализации этой атаки. Последнее делает более доступным аппаратное обеспечение исследований в этой области, в том числе в отечественной научной среде.

Детально изложенные в работе результаты анализа утечек информации обрабатываемой интегральным чипом по цепи электропитания значительно дополняет теоретический аппарат атаки, который может использоваться для разработки новых подходов для взлома аппаратно-реализованных защитных преобразований, а также и для поиска оптимальных путей их защиты.

Практическая значимость полученных научных результатов связана с тем, что предложенный метод защиты получил более полное обоснование по сравнению с другими известными программными методами защиты аппаратных реализаций шифрующих преобразований от побочных атак по цепям электропитания. Он имеет весьма широкую сферу практического применения и, прежде всего, для защиты аппаратных реализаций российских блочных шифров, применяемых в чипах электронных идентификационных документов, смарт-карт, а также микроконтроллерах, широко применяемых в промышленности.

Практическая значимость полученных научных результатов также подтверждается актом о внедрении от предприятия АО «Научные приборы» (г. Санкт-Петербург).

Полнота опубликованных результатов и соответствие паспорту специальности

По теме диссертации опубликовано 13 печатных работ, из них: 6 публикаций в изданиях, входящих в перечень рецензируемых научных изданий, рекомендованных ВАК Минобрнауки России; 6 публикаций в сборниках

научных статей и сборниках трудов научных конференций; 1 – отчет по НИР в АО «Научные приборы».

Основные результаты диссертационной работы достаточно полно представлены в научных публикациях соискателя и обсуждались на различных научно-технических конференциях и семинарах.

Работа выполнена в соответствии со следующими пунктами паспорта научной специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность:

– п. 3 «Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса»;

– п. 7 «Анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения»;

– п. 13 «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности».

Автореферат достаточно полно отражает содержание диссертации, в том числе полученные результаты, их новизну, практическую и теоретическую значимость, что позволяет получить по нему законченное представление о работе.

Замечания по диссертации и автореферату

1) Автор не указал в диссертации, преимущества предложенного им метода защиты в плане скорости выполнения защищённого им алгоритма защитного преобразования по сравнению с известными аналогами (методом маскировки и программной балансировки).

2) В качестве операций составляющих преобразования предобработки и постобработки, приведённого метода защиты, автор предлагает использовать многократную итерацию операций сложения по mod 2 и табличного преобразования. Данный подход кажется вполне разумным, однако возможны и другие варианты структуры построения процедур предобработки и постобработки, сравнение с которыми было бы полезным для обоснования выбранного решения. Проработка вопроса оптимизации (с точки зрения защищённости и скорости выполнения) структуры преобразований предобработки и постобработки выполнена не в полном объеме.
3) Исследование ограничено случаем российских стандартов на симметричные алгоритмы шифрования, тогда как вопрос о стойкости к атаке DPA стандарта цифровой подписи ГОСТ Р 34.10-2012 не изучался, хотя он также имеет высокую степень актуальности.
4) Вопрос экспериментального исследования стойкости блочных шифров «Магма» и «Кузнечик» к атаке DPA после встраивания предложенного механизма защиты их аппаратной реализации остался открытым.
5) В диссертации имеются отдельные неточности и опечатки (например, на странице 68 диссертации, после формулы (2.2) допущена описка – из формулы (2.2) понятно, что мощность получается из напряжения умножением на коэффициент 0.5, а не делением; в заключении к диссертации (пункт 4) на странице 203 допущена опечатка в окончании слова «восстановления»).

Заключение

Диссертация и автореферат содержат все требуемые разделы, а также оформлены в соответствии с п. 24.1 «Положения о совете по защите диссертаций на соискание учёной степени кандидата наук, на соискание учёной степени доктора наук», утверждённого приказом Министерства образования и

науки РФ от 13.01.2014 № 7. Содержание автореферата соответствует основным положениям диссертационной работы.

Отмеченные недостатки носят частный характер и не снижают высокой научной ценности и практической значимости проведённого исследования.

Диссертация Тихонова С.В. является законченной научно-квалификационной работой, в которой решена задача разработки метода обеспечения безопасности аппаратных реализаций защитных блоковых преобразований от побочных атак по цепям электропитания, имеющая существенное значение в области информационной безопасности.

Диссертационная работа соответствует критериям, установленным п.п. 9-14 Постановления Правительства РФ от 24 сентября 2013 г. № 842 «О порядке присуждения ученых степеней» (ред. от 28.08 .2017), а ее автор, Тихонов Сергей Владимирович, заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Официальный оппонент,
Заведующий лабораторией криптологии СПИИРАН
доктор технических наук, профессор

28 ноября 2017г. Молдовян Николай Андреевич

Подпись руки Молдовяна Николая Андреевича заверяю.

Начальник отдела кадров
СПИИРАН Д.В. Токарев

Сведения о составителе отзыва:

ФИО: Молдовян Николай Андреевич,
Ученая степень: доктор технических наук
Ученое звание: профессор
Место работы: Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН); почтовый адрес: 199178, Санкт-Петербург, 14-линия В.О., д. 39; www.spiiras.nw.ru ; телефон: (812) 328-34-11; эл. почта: spiiran@iias.spb.su
Должность: заведующий лабораторией криптологии
Рабочий телефон: (812) 328-51-85
Электронная почта: nmold@mail.ru