«УТВЕРЖДАЮ»

Проректор по научной работе СПбГЭТУ

Д.В.Гайворонский

«30» 11 2017 г.

ОТЗЫВ

на автореферат диссертационной работы 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»

На сегодняшний день широкую сферу применения имеют невскрываемые чипы, выполняющие некоторые защитные алгоритмы. Безопасность использования таких чипов критично зависит от возможности успешной реализации атак на выполняемые ими алгоритмы (в частности шифры). При этом недостаточно использовать современные шифры, устойчивые лишь к криптографическим атакам, так как существует класс атак, называемые побочными, которые позволяют извлечь секретные данные из невскрываемого чипа, анализируя его физические характеристики, такие как например энергопотребление (в частности атака DPA). Такие атаки позволяют весьма просто взломать незащищённые аппаратные реализации известных зарубежных шифров (например, 3DES, AES). Вопрос исследования подобных атак весьма важен, так как за счёт широкого распространения невскрываемых чипов, их защищённость имеет серьёзное значение для стабильности экономики и безопасности государства. Учитывая это диссертация Тихонова С.В., в которой производится исследование побочных атак по цепям электропитания, в том числе применительно к аппаратным реализация российских шифров

ГОСТ Р 34.12-2015, а также предлагается метод защиты от них является весьма важной и актуальной.

Судя по автореферату, соискателю удалось справиться с целями и задачами, поставленными в диссертации. В ходе проведённого исследования автором получены следующие основные научные результаты, выносимые на защиту:

1) Архитектура средства моделирования побочных атак по цепям электропитания. Модель «утечки» информации, обрабатываемой интегральным чипом, по цепи электропитания, основанная на результатах проведённого комплекса измерений.
2) Доказательство возможности успешного применения побочных атак по цепям электропитания к аппаратным реализациям шифров ГОСТ.
3) Метод защиты преобразований на интегральных чипах от побочных атак по цепям электропитания.

Новизна основных научных результатов состоит в том, что автором был рассмотрен ряд нераскрытых ранее аспектов реализации атак по цепям электропитания. При этом они имеют высокую важность как для проработки теоретического базиса атаки, так и при практических исследованиях. В том числе автор описал модель атаки DPA на российские шифры ГОСТ Р 34.12-2015, которую подтвердил на практике, проведя натурный эксперимент взлома шифра «Магма». Проведённые исследования позволили разработать новый метод защиты выполняемых чипом преобразований от атак типа DPA. Основной отличительной чертой этого метода является его универсальность – при помощи него могут быть защищены любые блочные шифры, в том числе и российские. Этот метод защиты реализуется дополнением программного кода, и не требует дополнительных усложнений чипа – может быть реализован даже на типовых микроконтроллерах. При этом обеспечивается относительно высокая скорость выполнения, и хорошая стойкость к атаке DPA, определяемая сложностью перебора дополнительного ключа.

Достоверность и обоснованность научных положений диссертации обеспечивается корректными теоретическими доказательствами, которые подтверждают проведённое компьютерное моделирование и натурные

эксперименты. Также необходимо отметить количество публикаций в рецензируемых журналах, апробацию результатов на международных конференциях и полученный акт о внедрении.

Судя по содержанию автореферата, работа отличается целостностью и завершенностью решения поставленных задач. Материал автореферата изложен ясно и дает представление о содержании выполненных исследований.

В качестве недостатка по автореферату хотелось бы выделить следующее:

1) В части автореферата, описывающей третью главу диссертации, даются результаты сравнения эффективности реализации DPA применительно к обоим российским блочным шифрам: «Магма» и «Кузнечик» (исходя из изложенного, сравнение осуществлялось аналитически). Однако далее описан натурный эксперимент, лишь для одного шифра – «Магма». Из доводов, приведённых в последнем абзаце раздела (15-я страница) можно допустить, что, эксперимент в отношении шифра «Кузнечик», не будет существенно отличаться. Однако, всё же необходимо было провести натурный эксперимент и в отношении шифра «Кузнечик», а если он был проведён, то его результаты стоило изложить в автореферате.
2) В автореферате нет полноценного сравнения предлагаемого решения с существующими, как зарубежными, так и отечественными. Для оценки потребительских свойств предлагаемого решения необходимо четкое понимание задач стоящих перед целевым заказчиком, а также четко сформулированный выигрыш, имеющий значение для целевого процесса реализуемого заказчиком, а не разработчиком предлагаемого решения.

Следует отметить, что отмеченные недостатки носят частный характер и не влияют на общее положительное мнение о выполненной работе.

Вывод:

Диссертация Тихонова С.В. является научно-квалификационной работой, в которой изложены новые решения, имеющие существенное значение для развития отрасли информационной безопасности в части реализации защитных преобразований, выполняемых интегральными чипами. Работа соответствует требованиям Постановления Правительства РФ от 24 сентября 2013 г. № 842 «О

порядке присуждения ученых степеней», а ее автор, Тихонов Сергей Владимирович заслуживает присвоения ему степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Заведующий кафедрой «Информационная безопасность»

Санкт-Петербургского государственного электротехнического

университета «ЛЭТИ» им. В.И. Ульянова (Ленина),

ктн, доцент Воробьев Евгений Германович

Наши реквизиты: Федеральное государственное автономное образовательное учреждение высшего профессионального образования “Санкт-Петербургский государственный электротехнический университет “ЛЭТИ” им. В.И. Ульянова (Ленина)” (СПбГЭТУ) Минобрнауки России, юр.адрес: ул. Проф. Попова, 5, С.-Петербург, 197376, Тел.: (812) 346-44-87, факс: (812) 346-27-58, E-mail: eltech@eltech.ru.