МИНОБРНАУКИ РОССИИ
федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого» (ФГАОУ ВО «СПбПУ»)

ИНН 7804040077, ОГРН 1027802505279, ОКПО 02068574

Политехническая ул., 29, С.-Петербург, 195251
Телефон (812) 297-20-95, факс 552-60-80
E-mail: office@spbstu.ru

22.11.2017 № 34/95

на № _____ **от** _____

Отзыв на диссертацию

Ученому секретарю
диссертационного совета
Д 999.121.03.
кандидату технических наук
А.Г. Владыко

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 весьма остро стоит вопрос обеспечения безопасности выполнения на интегральных чипах, аппаратно-реализованных защитных преобразований. И если их защищённость от криптографических атак сомнений не вызывает, то вопрос обеспечения их устойчивости к побочным атакам, в частности к атакам типа DPA, использующим утечку информации по цепи электропитания, является нетривиальным. С учётом этого тема диссертации и решаемая в ней научная задача по разработке метода, позволяющего обеспечить защиту аппаратных реализаций защитных блоковых преобразований от побочных атак по цепям электропитания

являются актуальными.

Судя по автореферату, при решении этой задачи автором получены три новых научных результата:

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.

В целом новизна полученных результатов состоит в развитии как теоретических, так и практических аспектов реализации побочных атак по цепям электропитания (в частности атаки DPA). Автор предложил оригинальную идею измерительной установки, позволяющей значительно снизить затраты на реализацию таких атак. Произвёл детальный анализ энергопотребления, взятого им для примера чипа, в частности зависимости энергопотребления от обрабатываемых им данных при выполнении различных операций. Учёт этих результатов будет весьма полезен для развития теоретических моделей атак по цепям электропитания. Далее автор подтвердил нестойкость российских шифров ГОСТ Р 34.12-2015 («Магма» и «Кузнечик») к атакам по цепям электропитания. В опубликованных на эту тему статьях автора и автореферате, впервые представлена модель атаки на эти шифры, а также приведены результаты натурного эксперимента. После этого автор предлагает метод защиты от атаки DPA. Он основан на оригинальной идее, обеспечивающей его универсальность – предлагается не вносить изменения в операции, составляющие алгоритм защитного преобразования, а совершать два дополнительных преобразования: одно перед выполнением алгоритма, а второе после него. Эти преобразования являются достаточно простыми, при этом снижение скорости выполнения алгоритма защитного преобразования является весьма небольшим.

Основной теоретической ценностью работы можно считать проведённое автором уточнение модели атак по цепям электропитания как представленными теоретическими доводами, так и практическими результатами исследования утечек информации по цепи электропитания. Практической ценностью работы, в первую очередь можно считать возможность использования предложенного метода защиты для обеспечения безопасности российских шифров ГОСТ, реализованных аппаратно.

Научные результаты работы могут быть использованы при выполнении перспективных НИР и ОКР, а также в учебном процессе при подготовке специалистов в области информационной безопасности.

Судя по автореферату, диссертация соответствует паспорту специальности 05.13.19. Результаты диссертации опубликованы в журналах из перечня, рекомендованного ВАК.

Недостатки:

1) На пятой странице автореферата над рисунком 1 говорится, что в диссертации сформулированы требования к полосе пропускания и чувствительности устройства сбора данных, однако эти требования даже кратко и тезисно не приводятся.
2) На десятой странице, стоило привести причины, по которым модель расстояния Хэмминга будет не эффективной, при анализе утечки от некоторых операций.
3) На 18-й странице автор пишет, что перебор 2^{48} вариантов ключа оказывается вычислительно нереализуемой задачей, а 2^{45} реализуемой с использованием мощных вычислительных ресурсов (например, суперкомпьютеров), что является несколько странным, поскольку разница в 8 раз не представляется чрезвычайно большой. В данном случае правильно было бы сказать, что перебор 2^{48} вариантов ключа является чрезвычайно трудно реализуемой задачей с точки зрения вычислений (а не невозможной).

Отмеченные замечания несколько снижают мнение о работе, но не ставят под сомнение новизну, значимость, обоснованность и достоверность

полученных научных результатов.

Вывод:

Судя по автореферату, диссертация Тихонова С.В. является законченной научно-квалификационной работой, по своей актуальности, глубине исследования, достоверности и обоснованности результатов, теоретической и практической значимости соответствует требованиям п. 9 Постановления Правительства РФ от 24 сентября 2013 г. № 842 «О порядке присуждения ученых степеней» (ред. от 28.08 .2017). Соискатель Тихонов Сергей Владимирович заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Директор Института физики, нанотехнологий и телекоммуникаций,
Доктор технических наук, профессор

Сергей Борисович Макаров

Санкт-Петербургский государственный политехнический университет
Института физики, нанотехнологий и телекоммуникаций
Санкт-Петербург, ул. Политехническая, д. 29, 2-й уч. корп.
Тел. (812) 552-95-16
director@phnt.spbstu.ru

Подпись Макарова С.Б.
УДОСТОВЕРЯЮ
Ведущий специалист
по кадрам
«27» 11