ОТЗЫВ

доктора технических наук, профессора Авсентьева Олега Сергеевича на автореферат диссертации 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

В автореферате Тихонова С.В. изложено, проведенное в диссертации исследование побочных атак по цепям электропитания на аппаратные реализации защитных блоковых преобразований. Анализ реализаций современных средств идентификации и аутентификации показывает, что их защищённость основывается на возможности безопасного выполнения некоторых защитных преобразований (например, таких как шифры) на аппаратных платформах, представляющих собой миниатюрные интегральные чипы. Применение таких известных шифров как AES, 3DES, ГОСТ гарантирует защищённость от известных криптографических атак. Однако, в настоящее время актуальными являются побочные атаки, использующие дополнительную информацию о выполняемом чипом алгоритме, утекающую, например, в цепи электропитания. Защититься от таких атак чрезвычайно сложно. Кроме того до настоящего времени не известны эффективные методы защиты от них шифров, реализующих алгоритмы в соответствии с ГОСТ. Указанные обстоятельства обуславливают актуальность темы диссертации, а также важность задач, решаемых в интересах достижения поставленной в ней цели.

В диссертации автору удалось решить ряд актуальных задач исследования реализации атак по цепям электропитания и, в частности, наиболее опасной из них – атаки на основе разностного анализа мощности (DPA). При реализации таких атак необходимо снимать данные об энергопотреблении интегрального чипа, представляющие собой сигнал с весьма малой амплитудой. В известных работах, авторы использовали дорогостоящее измерительное оборудование – широкополосный осциллограф со специальным пробником, усиливающим сигнал. Автор в своей работе предложил использовать существенно более дешевое оборудование – плату с аналого-цифровым преобразователем. При этом, в контексте реализации атаки

обеспечивается качество снимаемых данных не хуже, чем с использованием осциллографа. Автор исследовал зависимости энергопотребления чипа от обрабатываемых данных при выполнении различных операций. Результаты проведенного натурного эксперимента весьма важны, так как дополняют теоретическую модель атаки. Проведенные исследования позволили автору описать модель атаки DPA на российские шифры и реализовать в отношении них натурные эксперименты, доказать, таким образом, что шифры, реализующие алгоритмы ГОСТ (в незащищённом исполнении), не устойчивы к атакам DPA. Автор предложил оригинальный метод защиты от DPA, обладающий универсальностью (применим к защите любых блоковых шифров, в том числе ГОСТ Р 34.12-2015) и, вместе с тем, не требующий значительных дополнительных вычислительных ресурсов чипа.

Решенные вопросы, безусловно, обладают научной новизной, имеют теоретическую и практическую значимость. Достоверность результатов не вызывает сомнений, подтверждается строгими теоретическими доказательствами, компьютерным моделированием и результатами проведенных экспериментов.

По тексту автореферата целесообразно отметить следующие недостатки:

1. При обосновании актуальности темы, автор отмечает, что взлом выполняющегося на чипе защитного преобразования, по крайней мере, даст возможность сделать копию чипа. Однако, защитное преобразование рассматриваемого типа, является лишь частью выполняемой этим чипом программы. Например, такое преобразование может входить в состав протокола аутентификации, который, в свою очередь, повышая уровень агрегации, является лишь частью выполняемой чипом программы. При анализе устойчивости подобных чипов, в соответствии с принципом Кирхгоффа, когда атакующему данное защитное преобразование о нем известно все, кроме секретного ключа, доводы автора верны. Тем не менее, следует отметить, что на практике атакующему может быть неизвестна полностью выполняемая чипом программа. В этом случае при взломе защитного преобразования не получится изготовление полной копии чипа. Поэтому данный вопрос автору следовало бы конкретизировать.

2. На десятой странице, в таблице 1 приводятся характеристики зависимостей энергопотребления чипа от обрабатываемых данных для двух операций. Непонятно, почему для этих операций были взяты разные отсчеты

(например, для операции записи в ОЗУ взят 138-й отсчет, а для операции копирования данных между рабочими регистрами – 137-й).

Указанные недостатки не снижают ценность работы.

Вывод: Диссертация Тихонова С.В. является научно-квалификационной работой, в которой изложены новые обоснованные и доказанные решения, имеющие существенное значение для повышения безопасности инфокоммуникационных технологий в части реализации защитных преобразований, выполняемых интегральными чипами. Работа соответствует требованиям Постановления Правительства «О порядке присуждения ученых степеней», а ее автор, Тихонов Сергей Владимирович заслуживает присвоения ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Профессор кафедры информационной безопасности
Воронежского института МВД России,
доктор технических наук, профессор Авсентьтев Олег Сергеевич

Подпись Авсентьева О.С.
удостоверяю
начальник
делопроизводства
Воронежского института
МВД России Е.М. Долгих
05.12.2017

Почтовый адрес: Россия, Воронеж, 394065, Проспект Патриотов, дом 53.

Адрес электронной почты: ib@vimvd.ru

Телефон: +7 (473) 200-52-36.

Место работы: Федеральное государственное казенное образовательное учреждение высшего образования «Воронежский институт Министерства внутренних дел Российской Федерации».

Специальности д.т.н., профессора Авсентьева О.С.:

05.13.18 – Математическое моделирование, численные методы и комплексы программ;

05.13.19 – Методы и системы защиты информации, информационная безопасность.