

УТВЕРЖДАЮ
Заместитель начальника
Военно-космической академии
имени А.Ф. Можайского



О Т З Ы В

на автореферат диссертационной работы
Тихонова Сергея Владимировича
«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»

Широкое распространение методов аутентификации с использованием миниатюрных интегральных чипов делает актуальным вопрос обеспечения безопасности выполняемых ими алгоритмов. Основой методов аутентификации являются защитные преобразования информации с некоторым ключом, к примеру, шифры. При этом в подобных алгоритмах

применяются шифры, устойчивые к известным криптографическим атакам. Поэтому для взлома таких систем используются так называемые побочные атаки, которые позволяют получить из чипа дополнительную секретную информацию (утечку) путем анализа его физических параметров. Наиболее известной подобной атакой является разностный анализ мощности (DPA). На сегодняшний день побочные атаки, в целом, и атака по цепям электропитания, в частности, являются наиболее актуальными за счет того, что они позволяют наиболее эффективно извлекать секретную информацию из невскрываемых чипов. Защититься от таких атак крайне сложно, в частности, до сих пор не существовало эффективных методов защиты российских блочных шифров ГОСТ. Таким образом, задача исследования побочных атак по цепям электропитания и методов защиты от них является актуальной и востребованной для области информационной безопасности.

В своей работе автор рассматривает ряд нераскрытий ранее вопросов реализации атак по цепям электропитания и, в частности, DPA. Насколько можно судить из автореферата, автором впервые были детально описаны особенности зависимостей энергопотребления реального чипа от обрабатываемых им данных при выполнении разных операций. Автор показал весьма значительную сложность этих зависимостей, которую не учитывают существующие активно используемые теоретические модели атаки. Также была существенно дополнена теоретическая база атак DPA сравнением эффективности их реализаций, при которых используются подходы с расчетом ковариации и корреляции. Помимо аналитического описания были представлены результаты моделирования и практической реализации атаки с использованием снятых форм сигнала. Понимая особенности реализации DPA, а также анализируя структуру шифров ГОСТ Р 34.12-2015, было показано, что их незащищенные реализации (по аналогии с шифрами DES и AES) не будут устойчивы к DPA. Однако автор впервые представил детальную модель атаки на эти шифры и провел

натурный эксперимент по взлому аппаратно-реализованного шифра ГОСТ, что также является весьма заметным вкладом как в теоретическую, так и в практическую базу исследований атак по цепям электропитания. Наконец, была предложена новая идея по защите от атак типа DPA, причем данный подход является достаточно оригинальным. В отличие от существующих зарубежных методов защиты, предложенный в диссертации метод является, в целом, весьма универсальным и, что наиболее важно, подходит для защиты российских шифров ГОСТ. Более того, представленная автором реализация предложенного метода защиты предъявляет достаточно низкие требования к вычислительным ресурсам чипа и не требуется дополнительных аппаратных усложнений чипа.

Новизна полученных результатов не вызывает сомнений, а достоверность и обоснованность положений обеспечивается корректным использованием математического аппарата с подтверждением доводов результатами натурных экспериментов.

Вместе с тем, по автореферату можно отметить следующие недостатки:

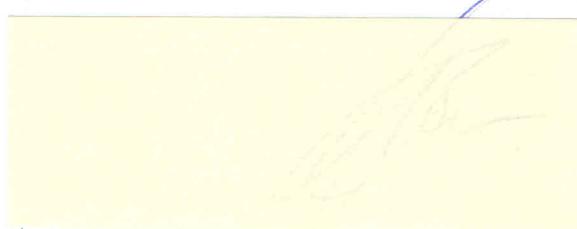
- 1) На представленных рисунками 2а и 4а формах сигнала сложно различить отличия их амплитуд при обработке комбинаций с разными весами Хэмминга.
- 2) В последнем абзаце восьмой страницы не раскрыта связь между потребляемой чипом мощностью (десятки мкВт) и требованиями к разрешению по напряжению у устройства сбора данных (100 мкВ).

Однако отмеченные недостатки, в целом, не снижают общего положительного впечатления от работы и не уменьшают ценности полученных теоретических и практических результатов. Анализ автореферата позволяет заявлять, что диссертация Тихонова С.В. является самостоятельным, завершенным научным исследованием, в котором содержится решение задачи, имеющей существенное значение для области информационной безопасности.

Вывод: Диссертация Тихонова С.В. на тему «Исследование и разработка модификаций аппаратно-реализованных защитных блоковых преобразований, устойчивых к побочным атакам по цепям электропитания» отвечает требованиям пунктов (п.п. 8, 9) «Положения о порядке присуждения ученых степеней», утвержденным постановлением Правительства РФ № 842 от 2013 г., предъявляемых к кандидатским диссертациям, а ее автор заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Отзыв рассмотрен на заседании кафедры, протокол от 07 декабря 2017 г., № 7.

Профессор кафедры
Систем сбора и обработки информации
кандидат технических наук, доцент
полковник



В. Зима

Наши реквизиты: Федеральное государственное бюджетное военное образовательное учреждение высшего профессионального образования «Военно-космическая академия имени А.Ф.Можайского» Министерства обороны Российской Федерации; адрес: ул. Ждановская, д. 13, г. Санкт-Петербург, 197198; тел. (812) 230-28-15; факс: (812) 237-12-49; e-mail: vka@mil.ru.