ОТЗЫВ

на автореферат диссертации Тихонова Сергея Владимировича «Исследование и разработка модификаций аппаратно-реализованных защитных блоковых преобразований, устойчивых к побочным атакам по цепям электропитания», представленной к защите на соискание учёной степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Известно, широкое применение информационно-телекоммуникационных систем и информационных технологий порождает появление новых информационных атак на защитные преобразования, осуществляемых на конкретном устройстве-чипе. Например, атаки простого и разностного анализа электропитания таких устройств (соответственно SPA и DPA). Такие атаки позволяют определить информацию, обрабатываемую чипом, в том числе и секретного ключа, реализованного на нем шифра. Поэтому тема диссертационной работы Тихонова С.В., посвященная разработке модификаций аппаратно-реализованных защитных блоковых преобразований, устойчивых к побочным атакам по цепям электропитания является актуальной.

Автором разработан программно-аппаратный комплекс для анализа «утечек», который позволил провести экспериментальное исследование «утечек» информации по цепям электропитания чипа. Доказано возможность применения побочной атаки по цепям электропитания аппаратных реализаций шифров РФ, частности «Магма» и «Кузнечик». Разработан метод защиты от побочных атак по цепям электропитания..

Новизна работы заключается в том, что впервые для снятия данных предложено использовать аналого-цифровой преобразователь, который позволил выявить особенности электропитания интегральных чипов, разработать модель побочной атаки по цепям электропитания на шифры РФ и универсальный метод защиты от таких атак.

Практическая значимость работы заключается в том, что разработанная модель «утечки» информации может быть использована для оценки возможных побочных атак по цепям электропитания при проектировании интегральных чипов, чтобы повысить методы защиты от таких атак.

В качестве недостатка следует отметить, что из автореферата неясно каким образом при выполнении эксперимента был реализован алгоритм сложения по mod2 и преобразования на S-box, выход которого выбирался в качестве промежуточного значения, а также, не совсем понятно, почему успешная атака на основе расчета корреляционных векторов требует меньшего количества форм сигнала.

Однако, указанные замечания, не влияют на полученные автором результаты. Проведенное исследование является законченной квалификационной работой, соответствующей требованиям Положения ВАК России, предъявляемым к кандидатским диссертациям. Ее автор Тихонов С.В. заслуживает присвоения ученой степени кандидата технических наук по специальности: 05.13.19 – Методы и системы защиты информации, информационная безопасность.

350010, г. Краснодар, ул. Зиповская, д.5, тел. 8(861) 252-30-31,
e-mail: kiiz@rambler.ru. НЧОУ ВО «Кубанский институт информзащиты».

Проректор по научной работе
доктор технических наук, профессор,
почетный работник высшего профессионального
образования Российской Федерации,
академик РАЕН Хисамов Франгиз Гильфанетдинович

24.11.17

Подпись профессора Хисамова Ф.Г. заверяю
заведующий канцелярией Татаренко Оксана Викторовна