На правах рукописи

Тихонов Сергей Владимирович

ИССЛЕДОВАНИЕ И РАЗРАБОТКА МОДИФИКАЦИЙ АППАРАТНО-РЕАЛИЗОВАННЫХ ЗАЩИТНЫХ БЛОКОВЫХ ПРЕОБРАЗОВАНИЙ, УСТОЙЧИВЫХ К ПОБОЧНЫМ АТАКАМ ПО ЦЕПЯМ ЭЛЕКТРОПИТАНИЯ

05.13.19 – Методы и системы защиты информации,
информационная безопасность

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2017

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» (СПбГУТ).

Научный руководитель: доктор технических наук, профессор
Коржик Валерий Иванович

Официальные оппоненты: **Молдовян Николай Андреевич**,
доктор технических наук, профессор,
федеральное государственное бюджетное учреждение науки «Санкт-Петербургский институт информатики и автоматизации Российской академии наук»,
заведующий лабораторией криптологии научно-исследовательского отдела проблем информационной безопасности

Левина Алла Борисовна,
кандидат физико-математических наук, доцент,
федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», доцент кафедры проектирования и безопасности компьютерных систем

Ведущая организация: Закрытое акционерное общество «Институт телекоммуникаций», г. Санкт-Петербург

Защита состоится 20 декабря 2017 года в 14.00 на заседании диссертационного совета Д 999.121.03 при федеральном государственном бюджетном образовательном учреждении высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский государственный университете аэрокосмического приборостроения», федеральном государственном бюджетном образовательной учреждении высшего образования «Балтийский технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова» по адресу 193232, Санкт-Петербург, пр. Большевиков, д. 22, корп. 1, ауд. 554/1.

С диссертацией можно ознакомиться в библиотеке СПбГУТ по адресу Санкт-Петербург, пр. Большевиков, д. 22, корп. 1. и на сайте www.sut.ru.

Автореферат разослан 17 ноября 2017 года.

Ученый секретарь
диссертационного совета Д 999.121.03,
канд. техн. наук А.Г. Владыко

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Безопасность современных информационно-коммуникационных систем неразрывно связана с алгоритмами, обеспечивающими конфиденциальность и целостность хранящейся и передаваемой информации, а также функции идентификации и аутентификации. Стойкость этих защитных преобразований, хоть и базируется на вычислительной сложности решения некоторых задач, но не может рассматриваться в отрыве от их практической реализации на конкретном устройстве – чипе. Относительно недавно стало известно, что физические параметры чипов, в частности энергопотребление, имеет явную зависимость от обрабатываемых ими данных. После чего, были предложены атаки простого и разностного анализа электропитания (соответственно атаки SPA и DPA), позволяющие использовать эту зависимость для взлома, выполняющихся на чипе защитных преобразований. Данный класс атак называют *атаками по побочным каналам* (или *побочными атаками*). В отличие от криптографических атак, которые используют уязвимости самих алгоритмов защитных преобразований, побочные атаки основываются на идее использования «утечки» информации о секретных данных, содержащихся в чипе, от его физических параметров. В идеале, они позволяют определить любую информацию, обрабатываемую чипом, вплоть до секретного ключа, реализованного на нём шифра. (В работе не рассматриваются криптографические методы взлома алгоритмов шифрования, а также методы разработки шифров для защиты от подобного рода криптоанализа. Поэтому можно обоснованно полагать, что в диссертации не исследуются методы криптографии.)

Чипы, выполняющие некоторые защитные преобразования, имеют широкую сферу применения в составе различных устройств, наиболее очевидные из них – это смарт-карты различного назначения и биометрические документы. Их защищённость критично зависит от стойкости, выполняемых чипом преобразований, таких как алгоритмы хеширования, ассиметричного и симметричного шифрования, а также других подобных методов. (Причём алгоритмы симметричного шифрования используются значительно интенсивнее остальных, поскольку они предъявляют наименьшие требования к, обычно, весьма сильно ограниченным аппаратным ресурсам чипа). Взлом, выполняющегося на чипе защитного преобразования, как минимум, даст возможность сделать копию чипа. Это, в свою очередь, сравнительно просто, позволит злоумышленнику подделать смарт-карту (используемую, например, в качестве ключа доступа или проездного документа), или нивелирует дополнительный уровень защиты, обеспечиваемый применением чипа в документе (например, в биометрическом паспорте).

С момента первых публикаций в 1999 году, эта тема активно разрабатывалась, в том числе предлагались разные по эффективности и простоте реализации методы защиты от атак такого типа. Однако результаты теоретических исследований оказывались недостаточно апробированы на практике, и в основном основывались на некоторых идеализированных моделях энергопотребления чипов. Поэтому оставался весьма актуальным вопрос проработки ряда практических аспектов реализации атаки, для того, чтобы учитывать их в используемых теоретических моделях. Кроме того, несмотря на чрезвычайную актуальность темы, до настоящего времени по ней существовало, крайне небольшое количество российских публикаций, что говорит о недостаточной разработанности этой темы в отечественной научной среде (по крайней мере в открытой её части). Это, в свою очередь, влечёт за собой и практические недоработки заключающиеся, например, в том, что зарубежные адаптации

известных программных методов защиты от побочных атак по цепям электропитания для аппаратных реализаций российских шифров (в частности «Магма» и «Кузнечик») оказываются мало эффективными, поскольку, изначально они разрабатывались преимущественно для шифров типа DES и AES.

Заключая вышесказанное, можно сделать общий вывод, что рассматриваемая тема имеет значительную актуальность не только в плане повышения общей её разработанности, но и в плане увеличения надёжности российских защитных преобразований.

Степень разработанности темы. Теоретические и практические аспекты реализации побочных атак по цепям электропитания разрабатывались с 1999-го года множеством зарубежных исследователей. Наиболее значимые работы, в плане проработки теоретического аппарата этих атак, принадлежат следующим авторам: S.Mangard, E.Peeters, M.Akkar, E.Brier, P.Kocher, T.Messerges. Значительный вклад в разработанность вопросов практической реализации атак внесли: J.Balasch, T.Eisenbarth, A.Moradi, D.Oswald. Наиболее действенные методы защиты предлагались следующими учёными: M.Akkar, J.Ambrose, A.Arora, J.Lv, F.Mace, M.Masoumi, D.May, A.Neve, G.Ratanpal, K.Tiri.

Несмотря на кажущуюся разработанность данной темы, даже в зарубежной литературе, остался целый ряд не раскрытых вопросов, как в части деталей практической реализации атаки, так и теоретических аспектов. Кроме того, существующие методы защиты от побочных атак по цепям электропитания были или слишком дороги в реализации, или обеспечивали защищённость аппаратных реализаций лишь небольшого числа зарубежных шифров. В частности, оставался открытым вопрос разработки дешёвого и надёжного метода защиты аппаратных реализаций российских шифров ГОСТ.

Цель и задачи исследования. Цель исследования состоит в повышении безопасности информационно-коммуникационных технологий в части реализации защитных преобразований, выполняемых интегральными чипами. Для достижения цели исследования в работе были поставлены и решены следующие частные задачи:

1) Разработка рациональной конструкции аппаратно-программного комплекса, предназначенного для анализа «утечек» информации по цепям электропитания (при ограничении стоимости используемого оборудования).

2) Экспериментальное исследование «утечек» информации по цепям электропитания интегрального чипа в зависимости от выполняемых им операций.

3) Оценка эффективности реализации побочных атак по цепям электропитания с проведением детального комплекса измерений.

4) Доказательство возможности применения побочной атаки по цепям электропитания на аппаратные реализации российских шифров.

5) Проведение сравнительного анализа сложности применения побочных атак по цепям электропитания к аппаратным реализациям шифров «Магма» и «Кузнечик».

6) Разработка универсального метода защиты от побочных атак по цепям электропитания (не зависящего от операций, составляющих защищаемый алгоритм и, в частности, применимого к аппаратным реализациям российских блочных шифров).

Объект исследования – аппаратно-реализованные защитные преобразования.

Предмет исследования – исследование теоретических и практических аспектов реализации атак по побочным каналам, использующих информацию, утекающую по цепи электропитания, а также разработка методов защиты от атак этого типа.

Научная (научно-техническая) **задача** – разработка метода, позволяющего обеспечить защиту аппаратных реализаций защитных блоковых преобразований от побочных атак по цепям электропитания.

Научная новизна.

1) В отличие от известных работ, для снятия данных об энергопотреблении чипа, вместо осциллографа, предложено использовать значительно более дешёвое и наилучшим образом подходящее оборудование – аналого-цифровой преобразователь.

2) В модели «утечки» информации учтены новые особенности энергопотребления интегральных чипов, выявленные в результате проведённого комплекса измерений.

3) Впервые представлена модель побочной атаки по цепям электропитания на аппаратные реализации обоих российских блочных шифров ГОСТ и произведён сравнительный анализ сложности её выполнения.

4) В отличие от других программных методов защиты, предлагаемый метод является универсальным (применим к защите любых аппаратно-реализованных защитных блоковых преобразований, в том числе российских шифров ГОСТ).

Теоретическая и практическая значимость работы.

Теоретическая значимость научных положений, изложенных в работе, состоит в следующем:

1) Расширен ряд аппаратных средств, позволяющих реализовать побочную атаку по цепям электропитания.

2) Дополнена модель, связывающая энергопотребление интегральных чипов с обрабатываемыми данными.

3) Расширена область применения побочных атак по цепям электропитания на аппаратные реализации шифров ГОСТ.

4) Расширен класс методов, обеспечивающих защиту преобразований на интегральных чипах от атак по побочным каналам.

Практическая значимость результатов проведенных исследований состоит в следующем:

1) Предлагаемая архитектура позволяет разработать измерительные системы на базе АЦП для решения задач анализа энергопотребления чипов при значительно меньшей стоимости чем существующие решения (базирующиеся на использовании осциллографа).

2) Модель «утечки» информации может быть использована в дальнейшем для оценки эффективности реализации побочных атак по цепям электропитания и методов защиты от них.

3) Представленная модель побочной атаки позволяет осуществить взлом аппаратных реализаций шифров ГОСТ за обозримое время. Модель может быть использована в дальнейшем для разработки методов защиты от подобной атаки.

4) Предложенный метод защиты обладает низкими требованиями к дополнительным аппаратным ресурсам чипа, простотой реализации и невысокой стоимостью.

Часть основных научных результатов реализована в АО «Научные приборы», по итогам чего получен акт о внедрении научных результатов. Внедрение результатов позволило:

– уточнить требования к разрабатываемым на предприятии электронным идентификационным документам;

– повысить надёжность функционирования производимого оборудования со встроенными блоками электронной идентификации.

Методология и методы исследования. Для решения поставленных задач использовались как общенаучные, так и специальные методы исследования, а именно аппарат

и методы алгебры и теории вероятности (в том числе корреляционный анализ), методология программирования (на языках низкого и высокого уровней), компьютерное моделирование, натурный эксперимент.

Положения, 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.

Степень достоверности результатов. Достоверность полученных результатов подтверждается строгими теоретическими доказательствами, компьютерным моделированием и результатами проведённых натурных экспериментов.

Апробация результатов. Основные результаты диссертационного исследования докладывались на Международной научно-технической и научно-методической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании» в СПБГУТ (Санкт-Петербург, 2013-2017), 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации» (Санкт-Петербург, 2015).

Публикации. Основные результаты диссертационного исследования опубликованы в 13-ти научных трудах, из них: 6 – в рецензируемых научных изданиях из Перечня ВАК; 6 – в сборниках научных статей, трудов, тезисов докладов и материалах конференций; 1 – отчет по НИР, АО «Научные приборы».

Личный вклад автора. Основные научные результаты получены автором самостоятельно в рамках, проведённых им, теоретических и экспериментальных исследований.

Структура и объем работы. Диссертационная работа состоит из введения, основной части (содержащей 4 раздела), заключения, списка литературы и приложений. Общий объем работы – 266 страниц, из них основного текста – 213 страниц. Работа содержит 118 рисунков и 31 таблицу. Список литературы включает 64 библиографических источника.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована важность и актуальность выбранной темы, определена цель и сформулированы решаемые в работе задачи. Перечислены новые научные результаты исследований, проведённых в рамках диссертационной работы, показана их теоретическая и практическая значимость.

В первой главе, на основе анализа известной литературы, даются основные сведения о побочных атаках по цепям электропитания.

Идея таких атак основана на физических особенностях строения и работы современных чипов. Их основные узлы (такие как, например: ПЗУ, ОЗУ, регистры) представляют собой связку логических вентилей (базовых элементов микросхемы, выполняющих элементарную логическую операцию). Логические вентили (ЛВ), состоят из полевых транзисторов,

связанных друг с другом в определённой последовательности. На примере работы простейшего ЛВ типа «НЕ» (инвертора), показывается, что большая часть его энергопотребления приходится на моменты переключения. Отсюда, энергопотребление чипа в целом зависит от количества изменивших своё значение разрядов в результате выполнения операций записи/чтения в/из ячейки ПЗУ, ОЗУ, регистров, а также от количества единиц в комбинациях, пересылаемых по шине данных и обрабатываемых в АЛУ. Приводятся основные используемые модели, позволяющие предположить энергопотребление чипа на основе информации об обрабатываемых им данных. Это модели расстояния Хэмминга и веса Хэмминга. Первая полагает, что энергопотребление чипа имеет пропорциональную зависимость от количества изменившихся бит в результате выполнения какой-либо операции. Вторая модель ограничивается лишь информацией о количестве единиц в обрабатываемой комбинации.

Затем описывается каждый элемент аппаратного комплекса (рисунок 1), необходимого для снятия данных об энергопотреблении такого качества, которое позволяет использовать их в дальнейшем для реализации побочной атаки по цепям электропитания. При этом формулируются требования к характеристикам его основного узла – устройства сбора данных (в роли которого обычно выступает осциллограф), в частности, требуемая полоса пропускания и чувствительность.

Рисунок 1 – Блок-схема измерительной установки

Наиболее тривиальной, является простая атака по цепям электропитания (SPA – Simple Power Analysis). Атака SPA предполагает прямую интерпретацию полученных данных об энергопотреблении чипа с целью идентификации отдельных выполняемых им операций, и даже определения обрабатываемых данных. Для этого, злоумышленник, с использованием тестового чипа (подобного анализируемому) определяет математическое ожидание и СКО значений отсчётов форм сигнала (рисунки 2а,б), характеризующих энергопотребление чипа при обработке комбинаций с различным весом (расстоянием) Хэмминга и выполнении разных операций (составляя таким образом некоторый шаблон, пример которого представлен на рисунке 2в, где $\mu(j,h)$ – математическое ожидание (характеризует полезную компоненту), а $\sigma(j,h)$ – СКО (характеризует шумовую компоненту) j-го отсчёта форм сигнала, при обработке комбинации с весом (расстоянием) Хэмминга равным h). Затем, сняв форму сигнала, характеризующую энергопотребление анализируемого чипа, выполняющего некоторый защитный алгоритм, он производит сопоставление амплитуды скачков его энергопотребления (в интересующей точке) с составленным шаблоном. Таким образом определяется вес (расстояние) Хэмминга данных, обрабатываемых чипом в соответствующий момент времени. Подобная атака позволяет использовать информацию «утекающую» по цепи электропитания чипа, например, для уменьшения количества возможных вариантов ключа блочного шифра до вполне переборных значений.

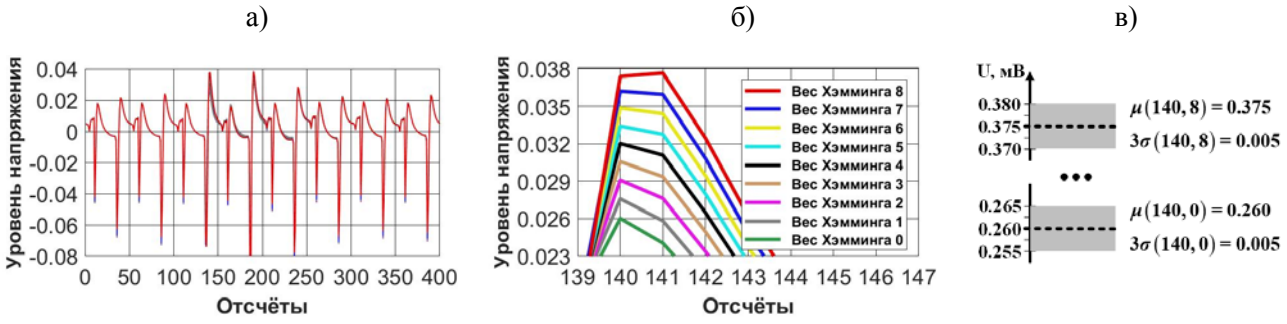

Рисунок 2 – Девять усреднённых (для минимизации шума) форм сигнала, полученных при пересылке комбинаций с различными весами Хэмминга, из регистра в чистую ячейку ОЗУ: а) полная форма сигнала; б) увеличенный участок с максимальным всплеском. в) Диаграмма математических ожиданий и СКО значений отсчёта для разных весов (расстояний) Хэмминга – шаблон SPA

Основными недостатками SPA можно считать необходимость детального знания особенностей реализации на чипе защитного алгоритма (в частности момента времени, в который обрабатывается интересующая злоумышленника комбинация) и весьма тривиальный метод защиты, заключающийся в зашумлении цепей питания чипа. Этих недостатков лишена значительно более эффективная, разностная атака по цепям электропитания (DPA – Differential Power Analysis). Она предполагает статистический метод анализа энергопотребления чипа, и применима в том случае, если злоумышленнику *доступно большое количество данных об энергопотреблении*. Для выполнения атаки DPA необходимо выбрать некоторое промежуточное значение алгоритма защитного преобразования $a_l(i) = f(m_l(i),\ k_l)$, которое можно рассчитать с использованием небольшой, l-й части (*подблока*) его ключа k и соответствующей части известных сообщений $m(i)$, $i = 1,\ ...,\ N$, где N – общее количество используемых сообщений. Затем снимаются формы сигнала, характеризующие энергопотребление чипа в процессе выполнения защитного преобразования (при этом выполняется N итераций с использованием случайных сообщений). После этого, для каждого варианта подблока сообщения $m_l(i)$ на d-м варианте перебираемого подблока ключа $k'_l(d)$, рассчитывается выбранное промежуточное значение $a'_l(i,\ k'_l(d))$, $d = 1,\ ...,\ D$, где D – общее количество вариантов перебираемого подблока ключа. Очевидно, что если вариант перебираемого подблока ключа был выбран верно: $k'_l(d) = k_l$, то для всех вариантов сообщений $m_l(i)$, значение $a'_l(i,\ k'_l(d))$ будет рассчитано верно: $a'_l(i,\ k'_l(d)) = a_l(i)$. В противном случае, за счёт однозначности операций, составляющих защитный алгоритм, значение $a'_l(i,\ k'_l(d))$ не будет совпадать с истинным. В зависимости от выбранной модели энергопотребления, рассчитывается вес Хэмминга значений $a'_l(i,\ k'_l(d))$ или расстояние Хэмминга между их значениями и предварительным заполнением ячейки, в которую производится запись результата: $h'_l(i,\ k'_l(d))$. После этого по формуле (1) определяется коррелированность рассчитанных значений $h'_l(i,\ k'_l(d))$ с каждым j-м отсчётом $b(i,\ j)$ снятых форм сигнала – таким образом для каждого варианта перебираемого подблока ключа $k'_l(d)$ строится корреляционный вектор. Очевидно, что корреляционный вектор, рассчитанный на истинном ключе, будет иметь всплеск значений в области, соответствующей

тем отсчётам форм сигнала, которые характеризуют энергопотребление чипа в момент обработки комбинации $a_l(i)$.

$$c\left(j,\ k_l'(d)\right)=\frac{COV\left(\vec{h_l'}\left(k_l'(d)\right),\ \vec{b}(j)\right)}{\sigma\left(\vec{h_l'}\left(k_l'(d)\right)\right)\cdot\sigma\left(\vec{b}(j)\right)}=$$

$$=\frac{\sum_{i=1}^{N}\left[h_l'\left(i,\ k_l'(d)\right)-\overline{\vec{h_l'}\left(k_l'(d)\right)}\right]\left[b(i,j)-\overline{\vec{b}(j)}\right]}{\sqrt{\sum_{i=1}^{N}\left[h_l'\left(i,\ k_l'(d)\right)-\overline{\vec{h'}_l\left(k_l'(d)\right)}\right]^2\cdot\sum_{i=1}^{N}\left[b(i,j)-\overline{\vec{b}(j)}\right]^2}},\qquad(1)$$

где $COV(A,\ B)$ – ковариация двух случайных величин A и B; $\sigma(A)$ – среднеквадратическое отклонение (СКО) случайной величины A; $\vec{b}(j)$ – вектор, состояний из N значений отсчёта $b(i,\ j)$; $j=1,\ ...,\ T$, где T – количество отсчётов из которых состоят снятые формы сигнала; $i=1,\ ...,\ N$, где N – общее количество обрабатываемых сообщений и, соответствующих им, снимаемых форм сигнала; $\vec{h_l'}\left(k_l'(d)\right)$ – вектор, состояний из N значений $h_l'\left(i,\ k_l'(d)\right)$ – веса (расстояния) Хэмминга промежуточного значения, рассчитываемого на d-м варианте перебираемого подблока ключа $k_l'(d)$; $d=1,\ ...,\ D$, где D – общее количество вариантов перебираемого подблока ключа; $\overline{\vec{A}}$ – среднее арифметическое по значениям элементов вектора $\vec{A}$.

Алгоритм повторяется для остальных подблоков ключа – в итоге ключ восстанавливается последовательно, по небольшим частям, с использованием дополнительной информации, утекающей по цепи электропитания чипа. Таким образом, побочная атака DPA, в отличие от теоретических атак (то есть криптографических методов взлома), имеет полиномиальную (а не экспоненциальную) сложность в зависимости от длины ключа защитного преобразования. При этом, в работе доказывается, что при увеличении количества обрабатываемых форм сигнала (накоплении статистики) формулу (1) можно привести к (2). Отсюда видно, что шумовая компонента (точнее значение её дисперсии) остаётся лишь в знаменателе формулы, а учитывая характеристики снимаемых форм сигнала, она оказывает незначительное влияние на успешность реализации атаки (рисунки 3).

$$c\left(j,\ k_l'(d)\right)\xrightarrow[N\to\infty]{}\frac{\Delta U_{\text{ДАН}}\cdot\left[\frac{1}{N}\sum_{i=1}^{N}\left(h_l'\left(i,\ k_l'(d)\right)\cdot h_l(i)\right)-16\right]}{\sqrt{2}\cdot\sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(h_l(i)\cdot\Delta U_{\text{ДАН}}\right)^2+\sigma\left(\xi(j)\right)^2-16\cdot\Delta U_{\text{ДАН}}{}^2}},\qquad(2)$$

где $\Delta U_{\text{ДАН}}$ величина, характеризующая изменение энергопотребления при каждом увеличении веса (расстояния) Хэмминга обрабатываемой комбинации на единицу; $h_l(i)$ – вес (расстояние) Хэмминга комбинации $a_l(i)$; $i=1,\ ...,\ N$, где N – общее количество обрабатываемых сообщений и, соответствующих им, снимаемых форм сигнала; $h_l'\left(i,\ k_l'(d)\right)$ – вес (расстояние) Хэмминга промежуточного значения рассчитываемого на d-м варианте перебираемого подблока ключа $k_l'(d)$; $d=1,\ ...,\ D$, где D – общее количество вариантов

перебираемого подблока ключа; $\xi(j)$ – значение шумовой компоненты j-го отсчёта форм сигнала; $j = 1, \ldots, T$, где T – количество отсчётов из которых состоят снятые формы сигнала; формула справедлива для чипов с 8-ми разрядной архитектурой.

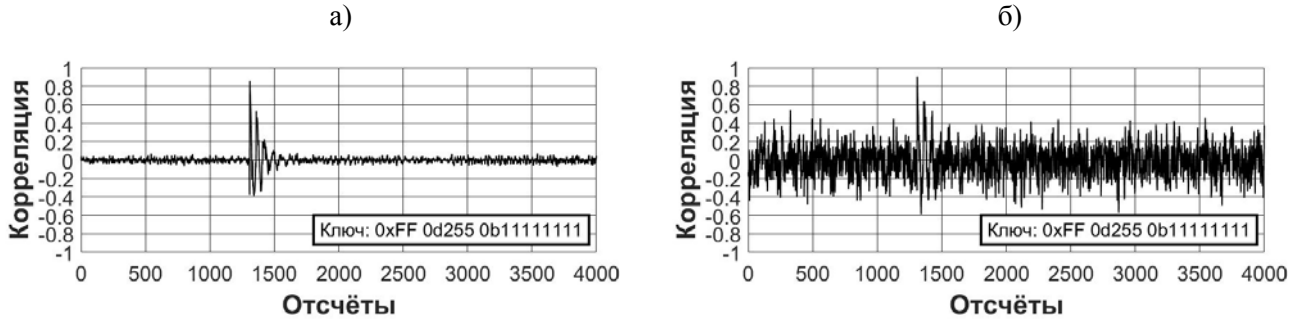

Рисунок 3 – Корреляционные векторы, полученные при реализации атаки DPA с использованием, в качестве рассчитываемого промежуточного значения, комбинации, записываемой в чистую ячейку ОЗУ, на истинном варианте ключа, при обработке: а) 2 000 форм сигнала; б) 30 форм сигнала

В последнем разделе главы приводится краткая характеристика основных методов защиты от DPA. Целью любого метода защиты является устранение зависимости значений отсчётов, снимаемых форм сигнала, характеризующих энергопотребление чипа, от обрабатываемых им секретных данных. Этого можно достичь внесением изменений в аппаратную составляющую чипа или в выполняемый им программный алгоритм. Методы, предполагающие дополнение или изменения аппаратной части чипа, на практике лишь снижают утечку информации по цепи электропитания, не устраняя её полностью, что нельзя считать надёжным способом защиты от DPA. Единственный такой метод, позволяющий полностью исключить «утечку» – аппаратная балансировка, предполагает реализацию защитного преобразования на чипах с многопроцессорной (в частности двухпроцессорной) архитектурой, что является весьма затратным. Программные методы защиты (такие как маскировка и программная балансировка) позволяют полностью устранить утечку информации, но они изначально создавались под конкретные алгоритмы зарубежных шифров, и, как показано в диссертации, их адаптация под российские шифры ГОСТ Р 34.12-2015 на практике является невозможной.

Во второй главе предлагается архитектура измерительной системы, предназначенной для снятия данных об энергопотреблении чипа, приводятся экспериментальные результаты анализа энергопотребления тестового чипа и оценка эффективности применения атаки DPA к восстановлению данных обрабатываемых на различных операциях.

При реализации атаки DPA требуется оборудование, позволяющее отличать амплитуды всплесков энергопотребления, вызванные обработкой комбинаций с разными весами (или расстояниями) Хэмминга. При этом различия в энергопотреблении чипа при обработке комбинаций, отличающихся одним разрядом, составляют порядка десятков мкВт (что предъявляет требования к разрешению по напряжению измерительной системы, порядка 100 мкВ). Поэтому в случае использования современных осциллографов (с 8-10 разрядными АЦП), авторы известных публикаций, дополнительно применяли специальные дорогостоящие пробники (усиливающие сигнал). При этом совокупная стоимость подобной установки превышает $10 000. В работе предлагается аппаратно-программный комплекс, в основе аппаратной части которого лежит не осциллограф, а значительно более дешёвая плата с 16-ти разрядным аналого-цифровым преобразователем фирмы Analog Devices. Причём совокупная

стоимость предложенной измерительной системы составляет менее $2 000, при этом обеспечивается требуемое разрешение по напряжению (порядка 60 мкВ) при достаточной полосе пропускания (до 150 МГц). В качестве анализируемого чипа был выбран весьма распространённый 8-ми разрядный микроконтроллер Atmel ATmega 16, монтаж которого на макетную плату осуществлялся таким способом, чтобы обеспечить максимальное качество снимаемых данных о его энергопотреблении.

С использованием описанной измерительной системы производился детальный анализ зависимостей энергопотребления от обрабатываемых чипом данных при выполнении таких операций как: чтение/запись из/в ОЗУ, чтение из ПЗУ, копирование данных между регистрами, операция сложения по mod2 (XOR). Результаты эксперимента подтверждают наличие чётко прослеживаемой зависимости между энергопотреблением чипа и обрабатываемыми им данными. Для примера, на рисунке 4а приведён участок форм сигнала, характеризующих энергопотребление чипа, при выполнении операции записи байта данных с разными весами Хэмминга в чистую ячейку ОЗУ (участок соответствует первому такту работы чипа, а всего, операция выполняется за два такта; увеличенная область этого графика с 139-го по 147-й отсчёты приведена на рисунке 2б). Затем, были построены гистограммы распределения значений 140-го отсчёта форм сигнала, в зависимости от веса Хэмминга обрабатываемой комбинации (на этом отсчёте форм сигнала наблюдается наибольший всплеск энергопотребления). Огибающие девяти гистограмм (по одной для каждого веса Хэмминга обрабатываемой комбинации) приведены на рисунке 4б. Отсюда чётко видно, что значение математического ожидания рассматриваемого отсчёта увеличивается с увеличением веса Хэмминга обрабатываемой комбинации, при достаточно стабильном значении СКО шума.

а) б)

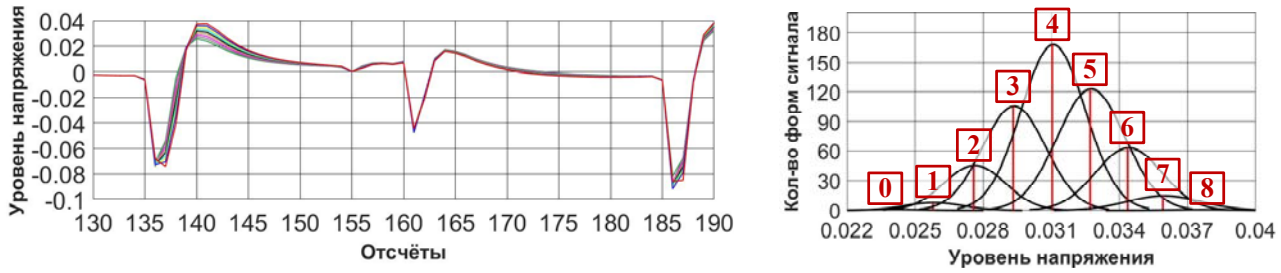

Рисунок 4 – а) Девять усреднённых форм сигнала для различных весов Хэмминга обрабатываемой комбинации, в рамках одного такта работы чипа; б) Огибающие гистограмм распределения значений 140-го отсчёта форм сигнала для каждого веса Хэмминга обрабатываемой комбинации (указан в квадратах)

Детальный анализ результатов экспериментов показал, что зависимости энергопотребления от обрабатываемых данных весьма далеки от идеальных теоретических моделей. Они имеют значительно более сложный характер, чем представлялось при изучении известной литературы. В качестве примера, в таблице 1 приведены части двух таблиц из приложения Е диссертации, в которых отражены основные характеристики зависимостей на разных отсчётах в рамках одного такта работы анализируемого чипа (пример участка формы сигнала изображён на рисунке 4а) при выполнении операции записи в ОЗУ и копирования данных между рабочими регистрами. Оттуда видно, что даже в рамках одного такта работы чипа на разных отсчётах: направление зависимости энергопотребления от веса Хэмминга

обрабатываемой комбинации может неоднократно меняться с прямой на обратную; имеются значительные отличия СКО шумовой компоненты; имеются значительные отличия величины $\Delta U_{\text{ДАН}}$.

Таблица 1 – Основные характеристики зависимостей энергопотребления от обрабатываемых данных на разных отсчётах в рамках одного такта работы анализируемого чипа

Операция	Зависимость	Отсчёт	$\Delta U_{\text{ДАН}}$, мВ	СКО, мВ	SNR
Запись в ОЗУ	Обратная	138	7.16	26.5	0.1752
	Прямая	141	2.73	2.55	2.8713
	Обратная	163	0.34	8.50	0.0038
	Обратная	172	0.44	1.62	0.1786
Копирование данных между рабочими регистрами	Обратная	137	2.47	36.8	0.0071
	Прямая	141	0.51	2.12	0.1457
	Обратная	163	0.26	8.36	0.0007
	Обратная	164	0.11	1.94	0.0030

Также выявлено, что зависимость энергопотребления от обрабатываемых данных существует не только на тех тактах работы чипа, на которых выполняется операция (в частности, рассмотренные операции выполнялись чипом за 1-2 такта), но и на 5-7-ми последующих тактах. (При этом значения $\Delta U_{\text{ДАН}}$ и СКО шумовой компоненты на разных тактах изменяются в широких пределах.) Так как чип выполняет операции строго последовательно без временных пропусков, то на всплески энергопотребления, вызванные выполнением одной операции, будут накладываться всплески от нескольких предыдущих операций, что является дополнительным шумом, затрудняющим реализацию атаки.

В изученных литературных источниках чётко разграничиваются случаи использования моделей веса и расстояния Хэмминга. В случае, если ячейка памяти, в которую сохраняется результат имеет предварительное заполнение, энергопотребление чипа должно иметь пропорциональную зависимость от количества разрядов, изменивших своё значение в результате перезаписи. Однако, экспериментальные исследования показали, что зависимость энергопотребления от веса Хэмминга обрабатываемой комбинации существует независимо от наличия предварительного заполнения ячейки назначения. Более того, учёт предварительного заполнения (использование модели расстояния Хэмминга) оказывается более эффективным лишь для операции чтения из ОЗУ в предварительно заполненную ячейку рабочего регистра. В то же время, к примеру, для операции записи в предварительно заполненную ячейку ОЗУ и операции чтения из ПЗУ в предварительно заполненную ячейку рабочего регистра, в принципе отсутствует зависимость между энергопотреблением и количеством изменившихся разрядов в ячейке назначения – существует зависимость лишь от веса Хэмминга обрабатываемой комбинации.

Также проведённый, анализ зависимостей энергопотребления чипа от обрабатываемых данных позволил дать рекомендации по параметрам требуемой измерительной установки. Оказывается необходимым обеспечить частоту дискретизации сигнала порядка 100 Мвыб/с, при разрешении по напряжению порядка 100-200 мкВ.

Затем, была выполнена атака DPA, для случаев, когда над рассчитываемым промежуточным значением совершались приведённые выше операции, в результате чего, для каждой рассмотренной операции, была дана оценка эффективности реализации атаки. Основным объективным критерием оценки эффективности DPA можно считать минимальное количество форм сигнала, после обработки которого, наибольшая амплитуда всплесков значений корреляционного вектора, рассчитанного на истинном ключе будет превышать всплески значений векторов, рассчитанных на ложных ключах (пример всплесков значений вектора, рассчитанного на истинном ключе изображён на рисунках 3). На практике, эффективность реализации DPA определяется двумя составляющими:

– статистическими характеристиками рассчитываемого промежуточного значения, в частности вероятностью совпадения его веса (или расстояния) Хэмминга, рассчитанного, с использованием случайных сообщений, на ложном варианте перебираемого подблока ключа, с истинным значением (чем эта вероятность больше, тем ближе друг к другу будут максимальные амплитуды всплесков значений корреляционных векторов, рассчитанных на истинном и ложных ключах, а значит потребуется обработать большее количество форм сигнала, для такого снижения влияния шумовой компоненты, которого будет достаточно для чёткого различения этих всплесков);

– отношением сигнал/шум, то есть отношением величины $\Delta U_{\text{ДАН}}$ к СКО шумовой компоненты – аналитические расчёты, подтверждённые экспериментально, показывают, что чем ниже шумовая составляющая по отношению к значению $\Delta U_{\text{ДАН}}$, тем меньшее количество форм сигнала необходимо обработать для однозначного определения корреляционного вектора, рассчитанного на истинном ключе, на фоне векторов, рассчитанных на ложных ключах, по максимальным амплитудам всплесков их значений (можно сказать, что отношение сигнал/шум, в определённом смысле, определяет объём информации «утекающей» по цепи электропитания).

При выполнении эксперимента, на анализируемом чипе был реализован алгоритм, состоящий из операции сложения по mod2 и преобразования на S-box, выход последнего выбирался в качестве рассчитываемого промежуточного значения: $a_l(i) = S\left(m_l(i) \oplus k_l\right)$, где $S(\cdot)$ – преобразование на S-box. Затем, над значением $a_l(i)$ совершались рассматриваемые операции. В этом случае, статистические характеристики рассчитываемого промежуточного значения были одинаковыми, и эффективность реализации DPA определялась объёмом информации «утекающей» по цепи электропитания, которая для рассмотренных операций весьма сильно отличается (пример для двух операций был приведён в таблице 1). В таблице 2 приведены приблизительные оценки минимального количества форм сигнала, требующегося для успешной реализации атаки, в случае совершения над рассчитываемым промежуточным значением некоторых из рассматриваемых операций. Отсюда очевидно, что эффективность реализации DPA для различных операций может отличаться на порядок. Также исследования показали, что большое значение имеет наличие предварительного заполнения ячейки и используемая в этом случае модель энергопотребления, так использование модели расстояния Хэмминга может требовать обработки на порядок большего количества форм сигнала (оказывается менее эффективной), чем в случае использования модели веса Хэмминга.

Таблица 2 – Минимальное количество форм сигнала, требующееся для успешной реализации атаки DPA, в случае расчёта корреляционных векторов, в зависимости от операции, совершаемой над рассчитываемым промежуточным значением

Выполняемая операция	**Состояние ячейки назначения**	**Минимальное количество форм сигнала, требующееся для успешной реализации атаки**
Запись в ОЗУ	Чистая	~30
	Заполненная	Однозначное определение ключа невозможно
Копирование из ОЗУ	Чистая	~410
	Заполненная	~560
Копирование из ПЗУ	Чистая	~160
	Заполненная	Однозначное определение ключа невозможно
Копирование между рабочими регистрами	Чистая	~25
	Заполненная	~170

В третьей главе приводится сравнение эффективности подходов к реализации атаки DPA, предполагающих расчёт корреляционных и ковариационных векторов, производится анализ отличий в эффективности применения DPA к отечественным шифрам «Магма» и «Кузнечик», а также выполняется экспериментальное исследование возможности взлома шифра «Магма», реализованного на анализируемом чипе.

Исторически первый подход к реализации DPA предполагал определять зависимость между рассчитанными на перебираемом подблоке ключа промежуточными значениями $a'_l(i,\ k'_l(d))$ и отсчётами снятых форм сигнала $b(i,\ j)$ при помощи расчёта ковариационных векторов. Впоследствии, вместо расчёта ковариации, исследователи начали применять корреляцию, однако сравнительный анализ эффективности реализации DPA с применением этих подходов в известной литературе не приводился.

Одним из важнейших достоинств атаки DPA, по сравнению с SPA (достигаемым использованием статистических методов анализа), можно считать отсутствие необходимости детального знания выполняемой чипом программы. Из алгоритма атаки DPA ясно, что наибольшие всплески значений корреляционных векторов, рассчитанных с использованием истинного варианта перебираемого подблока ключа, будут возникать в областях, соответствующих тем отсчётам форм сигнала, которые характеризуют энергопотребление чипа при обработке рассчитываемого промежуточного значения. В тоже время на корреляционных векторах, рассчитанных с использованием ложных вариантов ключа или в областях векторов, значения которых, соответствуют другим отсчётам форм сигнала, всплески будут иметь значительно меньшую амплитуду, за счёт существенно меньшей зависимости соответствующих отсчётов форм сигнала относительно значений рассчитываемой комбинации (по крайней мере, после статистического усреднения некоторого количества форм сигнала).

Аналитические расчёты, подтверждённые экспериментально показали, что при использовании выборок относительно большого объёма (десятки или даже сотни тысяч сообщений и соответствующих им форм сигнала) разница между всплесками на истинном и ложных вариантах ключа на ковариационных и корреляционных векторах будет приблизительно одинаковой. Но при использовании относительно небольших выборок чётко проявляется негативная особенность ковариации, заключающаяся в том, что последняя

характеризует не только степень зависимости двух случайных величин, но и разброс их значений (в контексте реализации DPA это значение величины $\Delta U_{\text{ДАН}}$, см. числитель в формуле (2)). Который на разных отсчётах форм сигнала может отличаться в весьма больших пределах, это приводит к появлению значительных «побочных» всплесков на ложных вариантах ключа, амплитуда которых может превышать амплитуду всплесков на истинном ключе. Было показано, также что амплитуда всплесков значений корреляционных векторов, несмотря на наличие нормировки, зависит как от значения $\Delta U_{\text{ДАН}}$, так и СКО шума, однако эта зависимость проявляется значительно меньше, поэтому успешная атака с расчётом корреляционных векторов возможна при использовании существенно меньшего количества форм сигнала (таблица 2 по сравнению с таблицей 3).

Таблица 3 – Минимальное количество форм сигнала, требующееся для успешной реализации атаки DPA, в случае расчёта ковариационных векторов, в зависимости от операции, совершаемой над рассчитываемым промежуточным значением

Выполняемая операция	**Состояние ячейки назначения**	**Минимальное количество форм сигнала, требующееся для успешной реализации атаки**
Запись в ОЗУ	Чистая	~550
	Заполненная	Однозначное определение ключа невозможно
Копирование из ОЗУ	Чистая	> 50 000
	Заполненная	~32 500
Копирование из ПЗУ	Чистая	> 50 000
	Заполненная	Однозначное определение ключа невозможно
Копирование между рабочими регистрами	Чистая	~3 500
	Заполненная	~12 000

Предложен алгоритм атаки DPA применительно к российским блочным шифрам «Магма» и «Кузнечик», а также исследованы статистические характеристики промежуточных значений этих шифров в разных точках (на разных этапах выполнения алгоритма). Теоретические исследования, подтверждённые моделированием, показали, что в контексте практической реализации рассматриваемых шифров на современных чипах, наибольшие отличия в эффективности применения к ним атаки DPA возникают в случае если в качестве рассчитываемого промежуточного значения выбирать выходы S-box. (Именно эта точка алгоритма шифра обычно и выбирается зарубежными авторами при реализации атаки DPA на такие шифры как DES и AES, поскольку она обладает наилучшими статистическими характеристиками, и при этом, выходы S-box, как-правило, можно рассчитать с использованием весьма небольшой части секретного ключа – от четырёх до восьми бит.) Выяснилось, что статистические характеристики выходов S-box шифра «Магма» оказываются несколько хуже (то есть такой шифр будет более устойчивым к атаке DPA), по сравнению с «Кузнечиком». Причиной этих различий является разрядность S-box – для шифра «Кузнечик» они 8-ми разрядные, а для «Магмы» – 4-х разрядные. При практической реализации S-box «Магмы» на чипах с 8-ми и более разрядной архитектурой, за одну итерацию будет осуществляться преобразование не над каждым S-box в отдельности, а сразу над парой S-box (рисунки 5), поскольку такой подход значительно эффективнее. При этом, соответствующий

скачок на снятых формах сигнала будет характеризовать энергопотребление, затрачиваемое на одновременную обработку всех восьми разрядов выходов этих двух S-box.

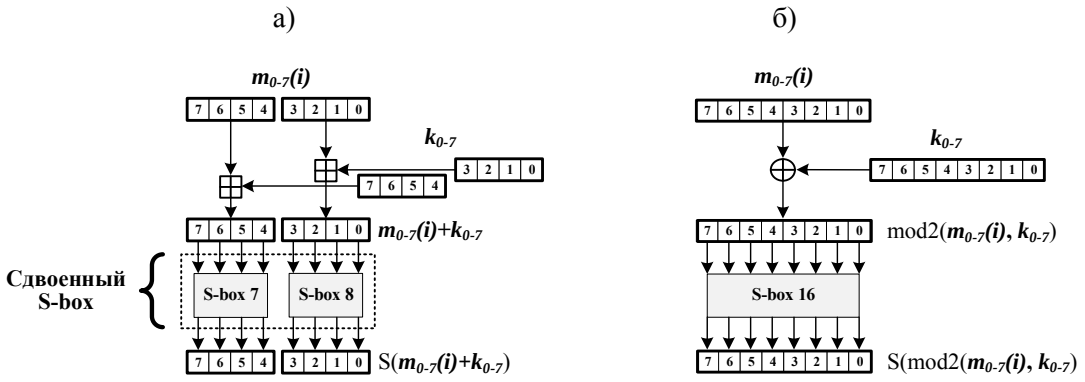

Рисунок 5 – Блок-схема части раунда: а) шифра «Магма»; б) шифра «Кузнечик»

Доказывается, что в контексте реализации DPA, статистические характеристики таких «сдвоенных» S-box значительно хуже, чем для «цельных» 8-ми разрядных S-box «Кузнечика». В частности, вероятность совпадения веса Хэмминга выхода, такого «сдвоенного» S-box, рассчитанного на ложных вариантах ключа, с истинным значением, может достигать 43.75%, тогда как для S-box «Кузнечика» – не более 29%. Однако, при прочих равных условиях, отличия статистических характеристик этих двух шифров не столь существенны чтобы считать, что один из них будет значительно устойчивее к атаке DPA, поскольку без применения специальных методов защиты, взлом обоих этих шифров, не составит сколько-нибудь значимого труда.

Была также произведена реализация шифра «Магма» на анализируемом чипе, особенности которой подробно описываются в работе. После этого в отношении представленной аппаратной реализации шифра была применена атака DPA, которая предполагала выполнение следующих шагов:

1) в процессе выполнения чипом алгоритма шифра, было снято $N = 5\ 000$ форм сигнала, характеризующих его энергопотребление, при шифровании случайных сообщений $m(i)$, $i = 1, \ldots, N$, причём каждая форма сигнала состояла из $T = 6\ 000$ отсчётов $b(i, j)$, $j = 1, \ldots, T$;

2) в качестве рассчитываемого промежуточного значения был выбран выход 7-8 S-box «Магмы»; его значение $a_l'(i, k_l'(d))$ рассчитывалось на ПК, для всех использованных сообщений на каждом варианте перебираемого 8-ми битового подблока ключа $k_l'(d)$, $d = 1, \ldots, 256$; в итоге для каждого варианта подблока ключа был составлен вектор $\vec{h_l'}(k_l'(d))$ элементы которого представляют значения весов Хэмминга рассчитанного выхода 7-8 S-box: $h_l'(i, k_l'(d))$, $i = 1, \ldots, 5000$, $d = 1, \ldots, 256$;

3) производился расчёт 256-ти корреляционных векторов $\vec{c}(k_l'(d))$, $d = 1, \ldots, 256$, при этом каждый элемент корреляционного вектора $c(j, k_l'(d))$, $j = 1, \ldots, 6\ 000$ характеризует зависимость между элементами вектора $\vec{h_l'}(k_l'(d))$ и элементами вектора $\vec{b}(j)$, образованного значениями каждого j-го отсчёта N форм сигнала.

В итоге корреляционный вектор, рассчитанный с использованием истинного варианта перебираемого подблока ключа, дал всплески значений, амплитуды которых превышали амплитуды всплесков, на корреляционных векторах, рассчитанных с использованием 255-ти ложных вариантов ключа (рисунки 6). Подобным же образом, не составило труда восстановить остальные части раундового ключа «Магмы».

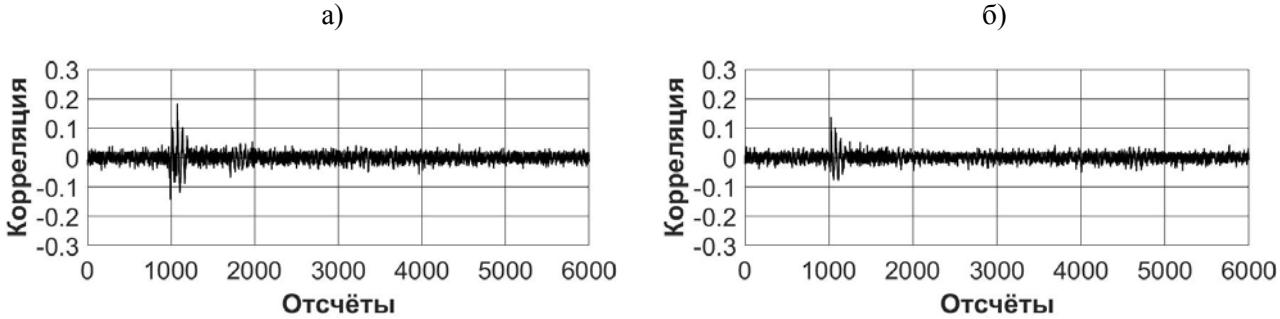

Рисунок 6 – Корреляционные векторы для случая, когда в качестве рассчитываемого промежуточного значения, выбирается выход 7-8 S-box «Магмы», на: а) истинном варианте перебираемого подблока ключа; б) наихудшем для злоумышленника ложном варианте перебираемого подблока ключа

На восстановление всего 256-ти битового секретного ключа «Магмы» ушло порядка шести часов, при этом, для расчёта корреляционных векторов, использовался ПК с весьма средней вычислительной мощностью.

Теоретические исследования, показали, что различные блочные шифры (как российские, так и зарубежные) имеют отличия в статистических характеристиках рассчитываемого промежуточного значения. Но они не столь значительны, как отличия в объёме «утекающей» по цепи электропитания, информации при выполнении разных операций. Поэтому, на основе полученных экспериментальных результатов можно сделать вывод, что, по большей части, эффективность реализации атаки DPA определяется не столько структурой анализируемого защитного преобразования, сколько его конкретной аппаратной реализацией.

В четвёртой главе предлагается новый подход к защите от DPA (рисунок 7а), который предполагает перед операцией защитного преобразования, реализуемой на чипе обычным (незащищённым) от DPA образом, производить защищённую от DPA предобработку входного сообщения с использованием некоторого *дополнительного* («непереборного») ключа, и такую же операцию производить с результатом выполнения защитного преобразования (для предотвращения возможности проведения атаки DPA начиная с последнего раунда).

На рисунке 7а: $m(i)$ – i-е входное сообщение; $P_{\mathrm{IN}}(\cdot)$, $P_{\mathrm{OUT}}(\cdot)$ – функции, описывающие преобразования соответственно предобработки и постобработки, с использованием дополнительного ключа k_{ADD}; $m'(i)$ – результат предобработки сообщения $m(i)$; $E(\cdot)$ – функция, описывающая преобразование комбинации $m'(i)$ на незащищённой реализации любого блокового защитного преобразования (например блочных шифров DES, AES, ГОСТ), с использованием секретного ключа k_{E}; $e'(i)$ – результат выполнения защитного преобразования; $e''(i)$ – комбинация $e'(i)$, после преобразования постобработки.

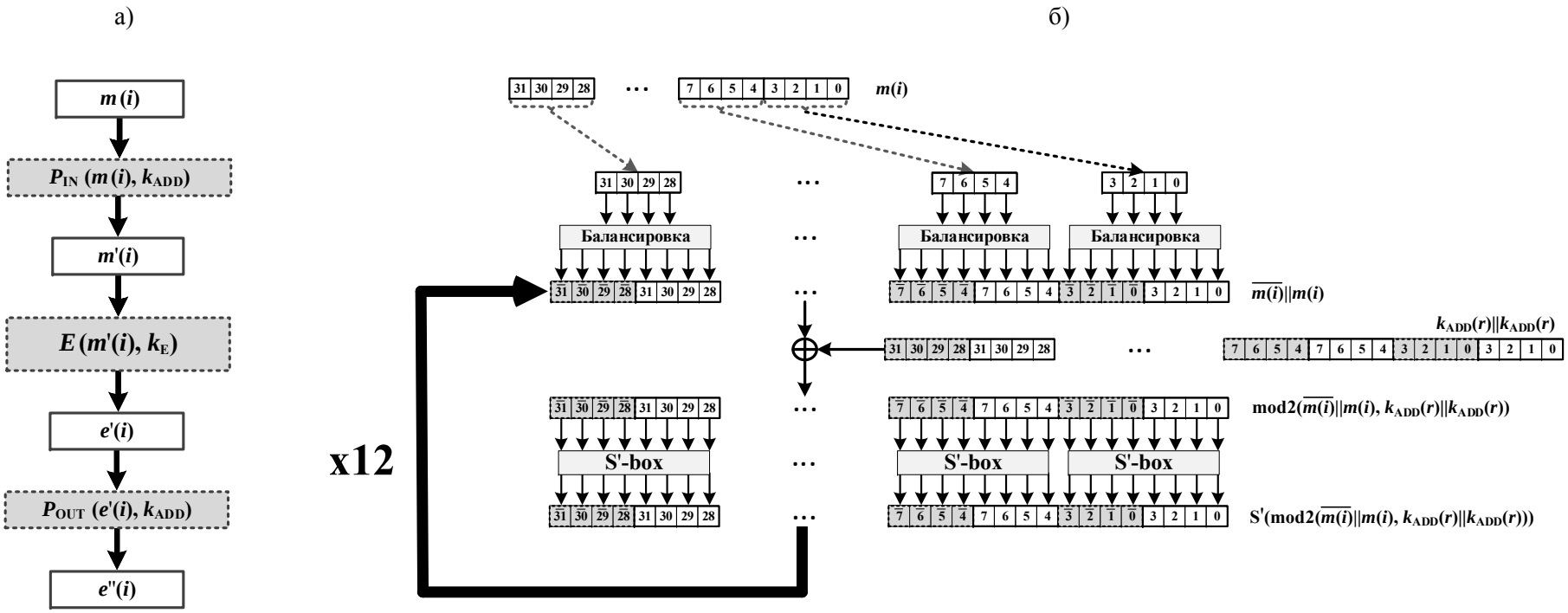

Рисунок 7 – Блок-схема предлагаемого метода защиты от DPA: а) общая структура; б) предлагаемая структура преобразований предобработки и постобработки

Преобразования предобработки и постобработки, должны обладать следующими тремя свойствами:

1) защищённость от DPA;

2) отсутствие возможности за разумное время произвести расчёт каких-либо бит комбинаций $m'(i)$ и $e'(i)$ только по известным комбинациям $m(i)$ и $e''(i)$;

3) однозначность и обратимость преобразований.

При соблюдении этих условий, злоумышленник окажется не в состоянии за реализуемое время найти биты входа $m'(i)$ или выхода $e'(i)$ защитного преобразования. Поэтому он не сможет произвести расчёт результата выполнения любых промежуточных операций защитного преобразования, путём перебора небольших частей его ключа. В результате атака DPA окажется невозможной.

Предлагается следующая структура преобразований предобработки (по аналогии и постобработки):

1) разбивка входа преобразования предобработки $m(i)$ на подблоки $m_l(i)$, $i = 1, ..., N$;

2) многократная итерация операции сложения по mod2 каждого подблока $m_l(i)$ с соответствующим подблоком дополнительного ключа $k_{\mathrm{ADD},\,l}(r)$, где r – номер итерации, и выполнение нелинейного преобразования;

3) склеивание подблоков, для последующей подачи полученной комбинации на вход защитного преобразования.

Для защиты от атак DPA операций сложения по mod2 и нелинейного преобразования предлагается использовать, представленный недавно группой австралийских учёных, метод называемый программной балансировкой. Идея этого метода основывается на особенности работы чипов с многоразрядной архитектурой (например: 8-ми или 16-ти разрядных), которая заключается в том, что, при выполнении операций над комбинациями, длина которых соответствует разрядности чипа, все их биты обрабатываются параллельно (одновременно). Поэтому, возможно определить энергопотребление, затрачиваемое чипом лишь на обработку комбинации в целом, а не отдельных её разрядов. Отсюда, предлагается такая модификация операций сложения по mod2 и нелинейного преобразования чтобы обрабатываемые комбинации, состояли из одинакового количества нулей и единиц (имели одинаковый вес Хэмминга). Это достигается за счёт одновременной обработки вместе с «полезной» (информационной) комбинацией, комбинации инвертированной к ней (балансирующей). Отсюда при любом значении информационных бит, балансирующие биты будут уравновешивать вес Хэмминга обрабатываемой комбинации, поддерживая таким образом энергопотребление чипа на постоянном уровне.

Предлагаемая структура преобразований предобработки и постобработки, состоящая из защищённых программной балансировкой, операций сложения по mod2 и нелинейного преобразования, представлена на рисунке 7б. При этом полагается, что используется чип с 8-ми разрядной архитектурой, а входной блок защитного преобразования имеет длину 32 бита. Хотя, такая структура может быть с лёгкостью адаптирована под чипы с большей разрядностью (например, под чипы с 16-ти разрядной архитектурой) и любую длину входного блока защитного преобразования. Применение криптографических атак для извлечения ключа преобразований предобработки и постобработки окажется невозможным ввиду того, что комбинации $m'(i)$ и $e'(i)$ злоумышленнику неизвестны. Реализация атак DPA с

использованием этих комбинаций принципиально оказывается возможной, но в процессе этого потребуется перебрать 2^{48} вариантов ключа (при чём, на каждом варианте, с использованием снятых данных об энергопотреблении, потребуется рассчитать корреляционный вектор), что на практике можно считать вычислительно нереализуемой задачей. В работе доказывается, что на чипах с 8-ми разрядной архитектурой бессмысленна реализация более 12-ти итераций преобразований, описанных рисунком 7б. Действительно, так как представленная структура преобразований предобработки и постобработки не является разветвлённой (отсутствует перестановка бит между l-ми подблоками), то совокупность преобразований каждого подблока можно представить в виде «чёрного ящика», после чего составить таблицу, где определённому значению входного подблока $m_l(i)$ (или $e_l''(i)$) будет ставится в соответствие значение выходного подблока $m_l'(i)$ (или $e_l'(i)$). Общее количество вариантов таких таблиц равно 16! (это число находится между 2^{44} и 2^{45}) – таким образом, вместо перебора ключа окажется легче совершить перебор вариантов таблиц (в этом случае, дальнейшее наращивание длины ключа, путём внесения дополнительных итераций является бессмысленным). В работе показывается, что перебор такого количества вариантов таблиц, в процессе реализации DPA, за обозримое время, будет возможным лишь в случае использования чрезвычайно мощных вычислительных систем (таких как, например, суперкомпьютеры). Наиболее тривиальный путь увеличения стойкости предлагаемого метода защиты состоит в использовании чипов с 16-ти разрядной архитектурой. В этом случае уже будет невозможно совершить перебор ключа или таблиц, за обозримое время (с использованием любых существующих или перспективных вычислительных комплексов).

Важно подчеркнуть, что использование предобработки и постобработки не затрагивает алгоритм защитного преобразования, поэтому его устойчивость к любым видам атак (в том числе криптографическим), оказывается не ниже структуры с незащищённой реализацией.

Одним из наиболее значимых качеств предлагаемого метода защиты является его универсальность – он не зависит от операций, составляющих алгоритм защитного преобразования, например, это может быть любой известный блочный шифр. При этом обеспечивается однозначность и обратимость преобразований. Более того, сам подход, заключающийся в выполнении преобразований предобработки и постобработки, не является строго определённым методом защиты. Разработчики могут предлагать различные структуры преобразований предобработки и постобработки, состоящие из оптимального сочетания операций, защищённых от DPA (различными методами), и при этом наилучшим образом подходящих для реализации на конкретном чипе.

Предложенный метод защиты был реализован автором на 8-ми разрядном микроконтроллере PIC для защиты шифра «Кузнечик», при этом скорость выполнения защитного преобразования снизилась приблизительно на 50% по сравнению с незащищённой реализацией (что является вполне хорошим результатом, так, например, известные реализации метода маскировки в отношении шифра AES снижают скорость шифрования в 2-4 раза, а балансировки – не менее чем в 2 раза), кроме этого потребовался примерно на 20% больший объём памяти программ (для хранения дополнительного кода программы, реализующего операции предобработки и постобработки), а также 256 байт памяти EEPROM для хранения дополнительного ключа и таблицы нелинейного преобразования. В целом, требования предложенного метода защиты к дополнительным аппаратным ресурсам чипа можно считать весьма небольшими по сравнению с известными аналогами.

ЗАКЛЮЧЕНИЕ

В диссертационной работе была решена научно-техническая задача по разработке метода, позволяющего обеспечить защиту аппаратных реализаций защитных блоковых преобразований от побочных атак по цепям электропитания.

В процессе решения частных задач исследования и, в соответствии с целевой установкой, были получены следующие основные результаты:

1) Предложен аппаратно-программный комплекс, позволяющий производить анализ «утечек» информации по цепи электропитания чипа и связанных с этим уязвимостей, реализованных на нём алгоритмов, при обеспечении минимальной стоимости по сравнению с известными аналогами.

2) Произведено экспериментальное исследование «утечек» информации по цепи электропитания анализируемого чипа в зависимости от выполняемых им операций. Дана оценка эффективности реализации DPA в отношении различных операций. Сделан ряд выводов об особенностях энергопотребления анализируемого чипа, влияющих на эффективность реализации атаки DPA.

3) Произведена сравнительная оценка эффективности подходов к реализации DPA, предполагающих расчёт ковариационных и корреляционных векторов. Доказывается, что на практике, эффективность применения подхода с расчётом корреляции, оказывается значительно лучше.

4) Описана теоретическая модель атаки DPA на аппаратную реализацию шифра «Магма», апробированная на практике, с использованием экспериментальных данных. В результате было доказано, что задача восстановления ключа «Магмы» может быть выполнена за обозримое время.

5) Произведён сравнительный анализ сложности применения DPA к аппаратным реализациям шифров «Магма» и «Кузнечик». Показано, что при их реализации на чипах с восьмью (и более) разрядной архитектурой, «Магма» окажется несколько более устойчивой к DPA по сравнению с «Кузнечиком».

6) Предложен новый метод защиты преобразований на интегральных чипах от побочных атак по цепям электропитания. При использовании этого метода, предъявляются достаточно низкие требования к дополнительным аппаратным ресурсам чипа, обеспечивается простота и не высокая стоимость реализации, а также строго доказанный уровень защищённости, определяемый вычислительной сложностью перебора дополнительного ключа.

Совокупность полученных научных результатов свидетельствует о достижении поставленной цели исследования – повышена безопасность информационно-коммуникационных технологий в части реализации защитных преобразований, выполняемых интегральными чипами.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ ПО ТЕМЕ ДИССЕРТАЦИИ

В рецензируемых научных журналах

1. Тихонов, С.В. О возможности взлома аппаратной реализации шифра ГОСТ / В.И. Коржик, С.В. Тихонов // Проблемы информационной безопасности. Компьютерные системы. – 2012. – № 3. – С. 53-62.

2. Тихонов, С.В. Метод защиты аппаратной реализации шифра ГОСТ от атаки измерения потребляемой мощности в цепи питания / С.В. Тихонов, В.И. Коржик // Проблемы информационной безопасности. Компьютерные системы. – 2013. – № 3. – С. 62-72.

3. Тихонов, С.В. Бесключевая криптосистема с обеспечением секретности на физическом уровне: миф или реальность? / В.И. Коржик, В.А. Яковлев, С.В. Тихонов // Проблемы информационной безопасности. Компьютерные системы. – 2015. – № 4. – С. 79-89.

4. Тихонов, С.В. Экспериментальное исследование утечек информации, обрабатываемой интегральными чипами, по цепи электропитания / С.В. Тихонов // Проблемы информационной безопасности. Компьютерные системы. – 2016. – № 1. – С. 82-93.

5. Тихонов, С.В. Экспериментальное исследование возможности взлома по цепям электропитания аппаратно реализованных блоковых шифров / С.В. Тихонов // Проблемы информационной безопасности. Компьютерные системы. – 2016. – № 2. – С. 106-117.

6. Тихонов, С.В. Универсальный метод защиты блочных шифров от побочных атак по цепям питания / С.В. Тихонов // Проблемы информационной безопасности. Компьютерные системы. – 2017. – № 3. – С. 63-73.

В других изданиях

7. Тихонов, С.В. Исследование методов защиты шифра ГОСТ от побочной атаки, использующей контроль потребляемой мощности / В.И. Коржик, С.В. Тихонов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2013): сборник научных статей II Международной научно-технической и научно-методической конференции. – 2013. – С. 829-831.

8. Тихонов, С.В. Разработка алгоритма предобработки аппаратно-реализованных блоковых шифров, обеспечивающих защищённость от атак DPA, при минимальных требованиях к аппаратным ресурсам / С.В. Тихонов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2014): сборник научных статей III Международной научно-технической и научно-методической конференции. – 2014. – С. 364-368.

9. Тихонов, С.В. Вторая революция в криптографии: миф или реальность? / В.И. Коржик, В.А. Яковлев, С.В. Тихонов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2015): сборник научных статей IV Международной научно-технической и научно-методической конференции: в 2 т. – 2015. – Т. 1. – С. 10-17.

10. Тихонов, С.В. Экспериментальное исследование взлома аппаратно реализованных блоковых шифров по цепям электропитания / С.В. Тихонов // Методы и технические средства обеспечения безопасности информации: Материалы 24-й научно-технической конференции 29 июня – 02 июля 2015 года. – 2015. – С. 100-102.

11. Тихонов, С.В. Исследование практической возможности взлома по цепям электропитания аппаратно реализованных шифров на примере ГОСТ 28147-89 /

С.В. Тихонов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2016): сборник научных статей V Международной научно-технической и научно-методической конференции: в 3 т. – 2016. – Т. 1. – С. 534-539.

12. Тихонов, С.В. Универсальный метод защиты блоковых шифров от побочных атак по цепям питания / С.В. Тихонов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2017): сборник научных статей VI Международной научно-технической и научно-методической конференции: в 4 т. – 2017. – Т. 2. – С. 652-654.

13. Тихонов, С.В. Исследование основных направлений создания средств и систем защиты электронных документов нового поколения: отчёт о НИР / М.М. Позднышев, А.Г. Бородинов, С.В. Тихонов [и др.]. – СПб.: АО «Научные приборы», 2014; инв. №231-АО от 16.11.2015 г. – 323 с.

Подписано в печать 18.10.2017. Формат 60x84 1/16.
Печ. л. 1,0. Тираж 70 экз.

Отпечатано в СПбГУТ, 193232, Санкт-Петербург, пр. Большевиков, д. 22, корп. 1