Алгоритм комбинирования акустического и электромагнитного каналов для осуществления атаки на RSA в программе GnuPG

К.С. Красов[1], А.Б. Левина [1]
[1]Санкт-Петербругский государственный электротехнический университет «ЛЭТИ»,
Россия, 197022, г. Санкт-Петербург

Аннотация. В данной статье рассматривается ускорение атаки по акустическому каналу на алгоритм RSA в программном обеспечении GnuPG за счёт устранения электромагнитных утечек. Сформулировано техническое обоснование целесообразности исследования. Особое внимание было уделено анализу взаимодействия акустических и электромагнитных сигналов, генерируемых устройством в процессе дешифрования с использованием RSA-4096. Выявлены характерные паттерны, соответствующие операциям дешифрования, на основе акустических и электромагнитных утечек. Представлены модели, демонстрирующие взаимодействие и возможности коррекции акустического сигнала с помощью данных, полученных из электромагнитных утечек. В результате была разработана модель атаки, позволяющая сократить время извлечения закрытых ключей, а также создан стенд и выполнены отдельные этапы атаки.

Ключевые слова: атаки по сторонним каналам, криптосистема RSA, акустические сигналы, электромагнитные сигналы, модуль регулятора напряжения.

Abstract. This paper investigates the acceleration of an acoustic channel attack on the RSA algorithm in GnuPG software through the elimination of electromagnetic leaks. The technical justification of the feasibility of the study is formulated. Particular attention is given to analyzing the interaction between acoustic and electromagnetic signals generated by the device during RSA-4096 decryption. Specific patterns corresponding to decryption operations have been identified from acoustic and electromagnetic leaks. Models demonstrating signal interaction and the potential for acoustic signal correction using data extracted from electromagnetic leaks are presented. As a result, an attack model was developed to reduce the private keys extraction time, a stand was developed, and separate stages of the attack were carried out.

Keywords: side-channel attacks, RSA cryptosystem, acoustic signals, electromagnetic signals, voltage regulator module.

Введение

Современные информационные системы сталкиваются с постоянно возрастающими угрозами безопасности, что делает защиту конфиденциальных данных одним из главных приоритетов в области кибербезопасности. Криптографические алгоритмы, такие как RSA, направлены на обеспечение конфиденциальности, целостности и доступности информации. Однако даже надёжные математические методы могут быть уязвимы для атак, использующих особенности физической реализации. Наибольшую опасность представляют атаки по сторонним (побочным) каналам, позволяющие извлекать секретные ключи за счёт анализа косвенных сигналов – акустических, электромагнитных или временных [1]–[3]. Особенно актуальны акустические атаки, поскольку они дают возможность удалённого сбора данных, снижая требования к физическому доступу злоумышленника к целевой системе [4], [5]. Значимость данного исследования усиливается в условиях активного распространения мобильных устройств и IoT-решений, для которых акустические и электромагнитные утечки становятся критическим вектором атак [6].

Одной из основополагающих работ в области атак по акустическим каналам является исследование Генкина, Шамира и Тромера [7], в котором была продемонстрирована возможность извлечения закрытых ключей RSA путём анализа акустических излучений, генерируемых в процессе вычислений в GnuPG. Авторы показали, что акустические излучения, генерируемые электронными компонентами компьютера во время операций умножения в алгоритме RSA, могут быть использованы для восстановления битов секретного ключа. В последующих исследованиях [8] был предложен улучшенный метод, использующий комбинацию акустических и электромагнитных каналов для повышения эффективности атаки. На основе теоретического моделирования было показано, что совместное использование рассмотренных каналов позволяет повысить точность восстановления битов секретного ключа и сократить время атаки. Разработанный алгоритм использовал электромагнитные утечки для коррекции акустических сигналов, что обеспечило сокращение количества необходимых итераций перехвата данных. Дополнительно была предложена модель, описывающая взаимосвязь энергопотребления процессора и акустических излучений, возникающих в ходе модульных операций.

Настоящее исследование направлено на экспериментальный анализ уязвимостей RSA в программном обеспечении GnuPG с использованием комбинации акустических и электромагнитных побочных каналов. Основное внимание уделяется разработке и проверке метода, позволяющего повысить эффективность обнаружения криптографических уязвимостей за счёт сокращения времени сбора и анализа данных. Предлагаемый подход предусматривает разработку системы, способной одновременно перехватывать и обрабатывать сигналы из обоих физических каналов, что даёт более полное представление о механизмах утечки информации. Полученные результаты позволяют глубже понять практические риски атак по побочным каналам и формируют основу для совершенствования мер защиты, а также для разработки методологических рекомендаций по созданию более устойчивых к подобным угрозам криптографических реализаций.

1. Криптосистема RSA и уязвимость акустического канала в GnuPG

1.1. Криптосистема RSA

Криптосистема RSA (Rivest-Shamir-Adleman) – это асимметричная система, предназначенная для обеспечения конфиденциальности и целостности данных. Она была предложена в 1977 году и стала основой для многих современных криптографических систем.

Процесс генерации ключей начинается с выбора двух больших простых чисел p и q, которые должны быть достаточно большими для обеспечения безопасности алгоритма. Затем вычисляется их произведение $n = pq$, которое используется в качестве модуля для обоих ключей. Далее определяется функция Эйлера:

$$\varphi(n) = (p-1)(q-1) \quad (1)$$

Данная функция необходима для вычисления открытого и закрытого ключей. После этого выбирается целое число e, удовлетворяющее условиям:

$$1 < e < \varphi(n) \quad (2)$$
$$e \perp \varphi(n)$$

Число e становится частью открытого ключа. Закрытый ключ d вычисляется как мультипликативная обратная величина к e по модулю $\varphi(n)$.

Сообщение m (где $m < n$) шифруется с использованием открытого ключа (e, n) по формуле:

$$c \equiv m^e \ (mod\ n) \quad (3)$$

где c – зашифрованное сообщение.

Для расшифровки зашифрованного сообщения c используется закрытый ключ (d, n) по формуле:

$$m \equiv c^d \ (mod\ n) \quad (4)$$

что позволяет восстановить исходное сообщение m.

Алгоритм RSA широко используется в различных областях, включая защиту данных в интернет-протоколах, а также в цифровых подписях, обеспечивающих подлинность и целостность сообщений.

1.2. Уязвимость акустического канала в GnuPG

GnuPG использует оптимизацию RSA на основе китайской теоремы об остатках (RSA-CRT). Данный метод значительно ускоряет операции дешифрования в алгоритме RSA. Вместо выполнения одной большой операции возведения в степень по модулю, RSA-CRT разбивает её на две меньшие операции, позволяя использовать два подмодуля p и q (где $n = pq$) для более эффективных вычислений.

Во время операций декодирования модуль регулятора напряжения (VRM) процессора генерирует акустические сигналы, которые могут содержать информацию о выполняемых вычислениях. Данные сигналы могут быть перехвачены специализированным оборудованием и проанализированы для извлечения сведений о внутреннем состоянии системы. В частности, акустические утечки могут содержать данные

о подмодулях, используемых в RSA-CRT, что делает возможным восстановление секретного ключа.

Кроме того, в реализации GnuPG существует особенность, заключающаяся в том, что последний бит подмодуля всегда равен 1. Это означает, что при анализе акустических утечек можно идентифицировать сигналы, соответствующие разным битам. Учитывая, что последний бит всегда фиксирован, можно определить, какие утечки соответствуют биту 1, а какие – биту 0. Это создаёт возможность для злоумышленника восстанавливать информацию о секретном ключе на основе анализа акустических сигналов.

Рассмотренный метод был подробно изучен в работе [7] и послужил основой для подхода, рассматриваемого в настоящем исследовании.

2. Разработка стенда для проведения эксперимента

Для оценки влияния комбинирования акустического и электромагнитного побочных каналов на эффективность атаки, необходимо разработать специализированный экспериментальный стенд. Такая установка позволит осуществлять контролируемый сбор данных и анализ утечек, генерируемых во время работы процессора, а также моделировать сценарии атак с использованием только акустического канала и их комбинации с электромагнитным.

Стенд состоит из двух основных подсистем: «жертвы» и «атакующего». «Жертва» представляет собой аппаратную платформу, выполняющую операции расшифрования в GnuPG, а «атакующий» отвечает за перехват и анализ акустических и электромагнитных сигналов.

Важным компонентом стенда является программный комплекс, синхронизирующий сбор данных из нескольких источников и обрабатывающий полученные сигналы для выявления корреляций между утечками и криптографическими операциями. Наличие такой структурированной экспериментальной среды позволяет системно оценить предложенную гипотезу о том, что объединение акустического и электромагнитного каналов может сократить время проведения атаки.

2.1. Разработка аппаратной части стенда

Успех атаки напрямую зависит от целевой платформы, так как для извлечения информации о закрытом ключе RSA необходимо перехватить утечки, генерируемые VRM процессора, реализация которого может значительно различаться в зависимости от материнской платы (например, некоторые дроссели издают больше шума, чем другие [9]).

По этой причине перед проведением атаки крайне важно подобрать подходящий компонент системы, который будет использоваться в качестве имитации жертвы.

Конкретным критерием пригодности является то, что система считается уязвимой, если при расшифровке различных файлов, зашифрованных одной и той же парой ключей, формируются сигналы, различающиеся по частоте.

Для эксперимента были выбраны следующие устройства:

- Материнская плата Gigabyte GA-G31M-S2L;
- Материнская плата Gigabyte GA-P41-ES3G;
- Материнская плата Asus P7P55LX;
- Ноутбук HP ProBook 455 G6 (версия AMD Ryzen 2700u).

Выбор обусловлен их фактической доступностью. Также стоит отметить, что данный набор охватывает несколько поколений и различных производителей процессоров, но объединён архитектурой x86.

На примере материнской платы Gigabyte GA-G31M-S2L было протестировано влияние корпуса дросселя на качество получаемой акустической утечки. На рисунке 1 показан незакрытый дроссель.

Рисунок 1 – Незакрытый дроссель

Для сравнения были зафиксированы акустические утечки при расшифровке файла до снятия кожуха дросселя и после. Результаты представлены на рисунке 2.

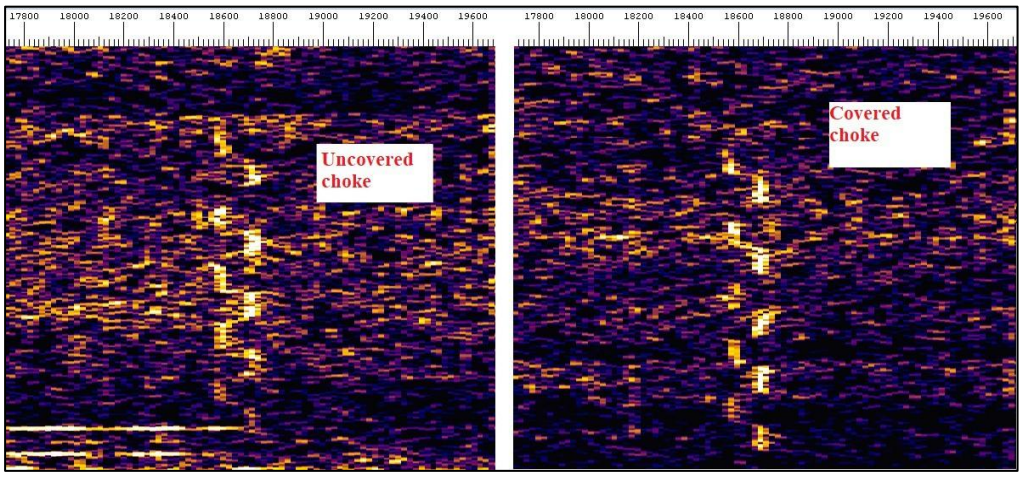

Рисунок 2 – Акустические утечки для незакрытого и закрытого дросселей

Из рисунка 2 видно, что шаблон, соответствующий процессу расшифрования, чётко прослеживается как слева, так и справа, что говорит о том, что снятие кожуха лишь незначительно улучшает сигнал. Однако данная материнская плата не удовлетворяет ранее определённому критерию и была исключена из дальнейшего анализа.

Среди представленных вариантов наиболее подходящей оказалась материнская плата Asus P7P55LX. На рисунке 3 показаны дроссели VRM данной материнской платы.

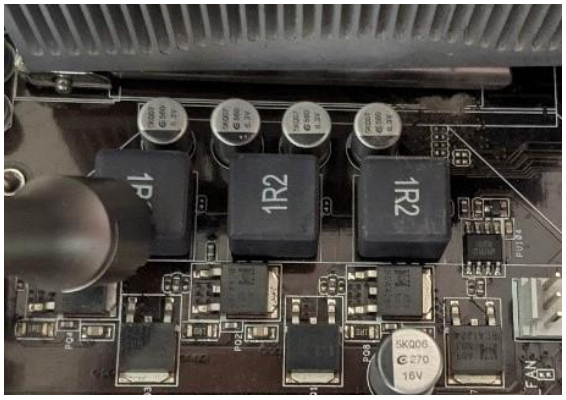

Рисунок 3 – Дроссели VRM на Asus P7P55LX

На рисунке 4 показаны акустические утечки, полученные в процессе расшифровки на данной материнской плате.

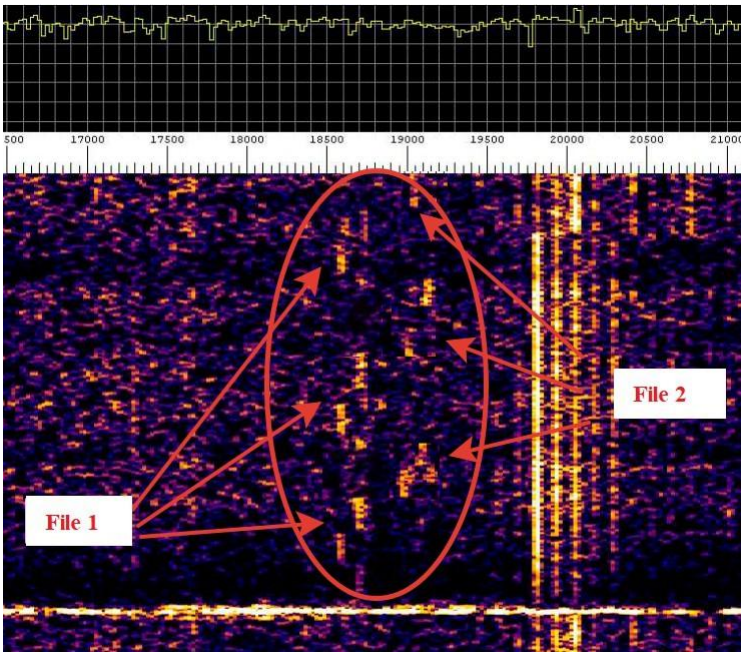

Рисунок 4 – Акустические утечки, полученные с помощью Asus P7P55LX

Блок питания и жёсткий диск были изолированы от основного стенда, поскольку они содержат механические элементы, создающие шум. Данные шумы не влияют на результативность атаки, однако их устранение требует дополнительных ресурсов, что не является предметом данного исследования – поэтому при проведении лабораторных экспериментов шумы были устранены.

На основе выбранных компонентов был создан экспериментальный стенд. В дополнение к материнской плате использовались:

- Микрофон ProAudio PMC-2;
- Внешний звуковой интерфейс Creative E-MU 0404-USB;
- Приёмник электромагнитных утечек на основе Arduino с катушкой и усилителем.

Структурная схема разработанного стенда представлена на рисунке 5.

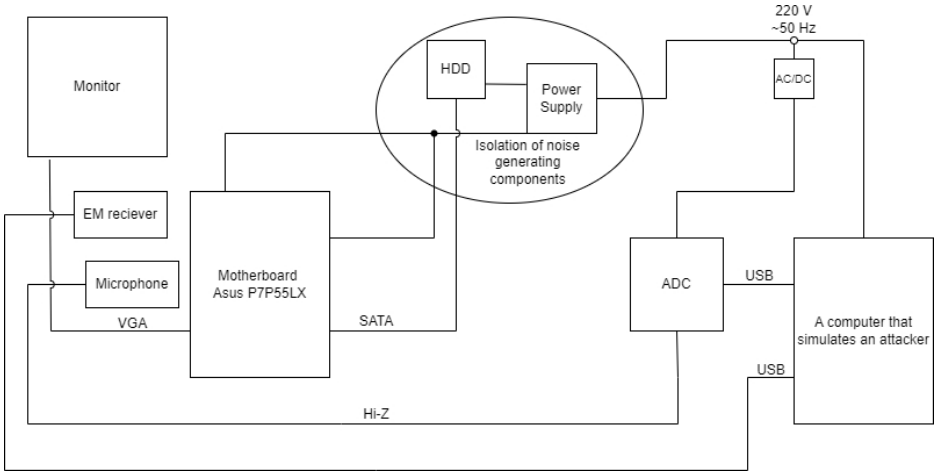

Рисунок 5 – Структурная схема разработанного стенда

2.2. Разработка аппаратной части стенда

В данной работе применяется метод коррекции акустического сигнала с использованием электромагнитного сигнала в качестве эталонного. Суть метода заключается в вычитании из акустического сигнала разности между акустическим и электромагнитным сигналами, что позволяет усилить компонент, соответствующий электромагнитным утечкам, и ослабить помехи, вызванные источниками акустического шума.

Коррекция сигнала выполняется по формуле:

$$S_{corr}(t,\alpha) = S_{ac}(t) - \alpha\big(S_{ac}(t) - S_{em}(t)\big) \tag{5}$$

где $S_{corr}(t,\alpha)$ – скорректированный сигнал,
$S_{ac}(t)$ – акустический сигнал,
$S_{em}(t)$ – электромагнитный сигнал,
α – весовой коэффициент, определяющий степень корректировки.

Значение α определяется экспериментально и может варьироваться в зависимости от аппаратной платформы и условий проведения эксперимента.

Вышеприведенное выражение можно переписать в виде:

$$S_{corr}(t,\alpha) = (1 - \alpha)S_{ac}(t) + \alpha S_{em}(t) \tag{6}$$

Таким образом, итоговый сигнал является комбинацией исходных акустического и электромагнитного сигналов, а параметр α управляет уровнем корректировки.

Весовой коэффициент α играет ключевую роль, поскольку он определяет, насколько точно акустический сигнал будет скорректирован с учётом электромагнитного. Для определения оптимального значения α были рассмотрены два подхода: оптимизация по метрике «сигнал/шум» (SNR) и метод минимизации ошибки с использованием опорного сигнала.

Метод SNR предполагает, что оптимальный коэффициент α выбирается исходя из максимизации отношения сигнал/шум после коррекции. В данном случае задача сводится

к поиску такого значения α, при котором полезный сигнал максимально усиливается, а шум, неизбежно присутствующий в реальных условиях, минимизируется.

В рассматриваемом контексте полезным сигналом считается скорректированный сигнал $S_{corr}(t,\alpha)$, а под шумом $N(t,\alpha)$ понимается разница между исходным акустическим и скорректированным сигналом. Таким образом, шум определяется как:

$$N(t,\alpha) = S_{ac}(t) - S_{corr}(t,\alpha) \tag{7}$$

Подставляем выражение (5), получаем:

$$N(t,\alpha) = \alpha\big(S_{ac}(t) - S_{em}(t)\big) \tag{8}$$

При наличии временной зависимости сигналов целесообразно определять SNR через интегральные характеристики по всему временному интервалу T. Тогда $SNR(\alpha)$ записывается в следующем виде:

$$SNR(\alpha) = \frac{\int_T [S_{corr}(t,\alpha)]^2 dt}{\int_T [N(t,\alpha)]^2 dt} \tag{9}$$

Подставляем полученные ранее выражения:

$$SNR(\alpha) = \frac{\int_T [(1-\alpha)S_{ac}(t) + \alpha S_{em}(t)]^2 dt}{\alpha^2 \int_T [S_{ac}(t) - S_{em}(t)]^2 dt} \tag{10}$$

Оптимальное значение весового коэффициента α выбирается на основе максимизации SNR:

$$\alpha_{opt} = arg\max_{\alpha} SNR(\alpha) \tag{11}$$

Для сравнения сигналов во времени применялся метод взаимной корреляции. Кросскорреляционная функция $R(\tau)$ определяется как:

$$R(\tau) = \int_T S_{ac}(t) S_{em}(t+\tau) dt \tag{12}$$

где τ – временная задержка.

Максимум функции $R(\tau)$ соответствует оптимальной синхронизации сигналов, то есть значению τ_{max}, при котором акустический и электромагнитный сигналы наиболее коррелированы. Определение временной задержки позволило не только скорректировать смещение между сигналами, но и повысить эффективность последующей обработки данных, включая выбор оптимального значения весового коэффициента α.

Программная часть реализована под Microsoft Windows 10, что связано с тем, что связано с наличием драйвера для используемой звуковой карты только для данного семейства систем.

Для реализации программной части были выбраны следующие инструменты:

- Язык программирования C++;
- Библиотека FFTW3;
- Библиотека libconfig.

На рисунке 6 показана диаграмма классов разработанной программы.

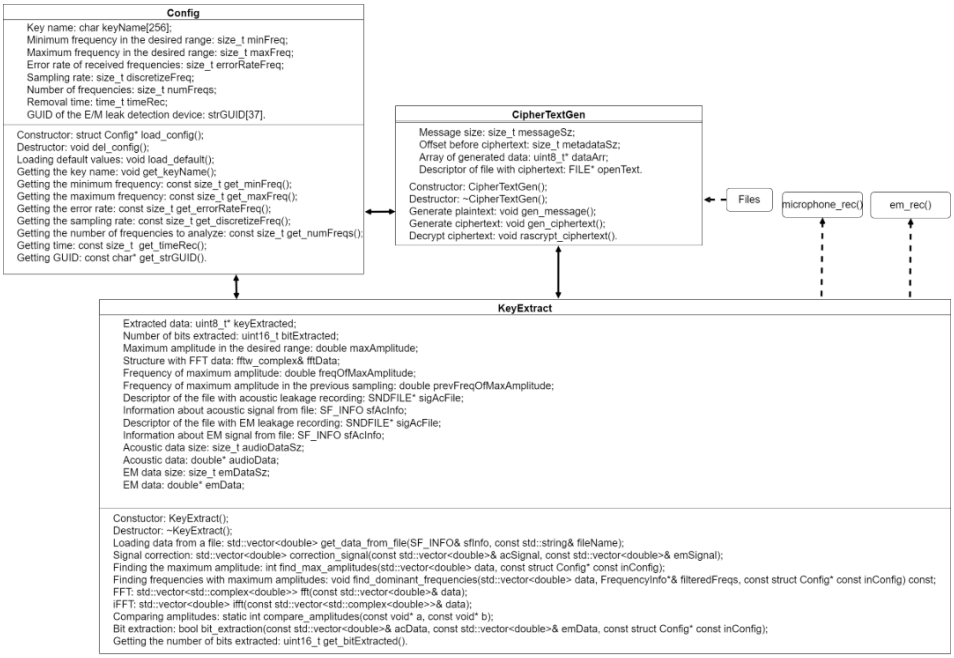

Рисунок 6 – Диаграмма классов разработанной программы

Разработанная программная часть позволила автоматизировать процесс атаки. Реализация включает модули настройки параметров, регистрации акустических и электромагнитных утечек, генерации модифицированных шифротекстов с учётом особенностей механизма проверки целостности GnuPG [10], а также анализа полученных данных, включающего быстрое преобразование Фурье, частотную фильтрацию и коррекцию сигнала. На основе полученных данных возможно восстановление закрытого ключа RSA с применением атаки Копперсмита [11]. Также реализована демонстрационная версия, позволяющая визуализировать работу без проведения реальной атаки. В сочетании с описанной ранее аппаратной частью стало возможным проведение эксперимента.

Таким образом, использование скорректированного сигнала упрощает выявление характерных шаблонов. При использовании только акустического подхода некоторые зафиксированные трассы могут интерпретироваться неоднозначно. В таких случаях злоумышленнику приходится повторно отправлять файл на расшифрование, снова запускать GnuPG, захватывать новые трассы и анализировать их. По мере извлечения большего числа битов ключа правильное определение каждого следующего бита становится всё сложнее, что приводит к увеличению количества итераций цикла «расшифровка–захват–анализ». После применения коррекции сигнала доля неоднозначных трасс заметно снижается, что уменьшает число полных итераций и сокращает общее время атаки.

3. Эксперимент

Для оценки эффективности предложенного алгоритма комбинирования акустического и электромагнитного каналов при атаке на RSA в GnuPG был проведён эксперимент, в котором сравнивалось время выполнения атаки по новому методу с исходным подходом.

3.1. Условия и методика эксперимента

В качестве тестовых данных было сгенерировано пять пар ключей RSA-4096. Для каждой пары ключей было проведено десять измерений. В результате было получено 50 значений времени, затраченного на проведение атаки ($N = 50$ [12]).

Эксперимент проводился в лабораторных условиях. Стенд, имитирующий атакуемую систему, был собран таким образом, чтобы исключить шум от компонентов компьютера. Оборудование, используемое для фиксации утечек, было предварительно откалибровано для обеспечения точности измерений.

Акустическая обстановка в лаборатории характеризовалась уровнем фонового шума, измеряемого в диапазоне 35-40 дБ, с преобладанием низкочастотных составляющих, обусловленных работой вентиляционной и кондиционерной систем, а также фоновым шумом от электронного оборудования, находящегося в помещении. На принимаемые электромагнитные сигналы основное влияние оказывал сам стенд, тогда как остальная часть обстановки практически не влияла на результаты.

Для каждого набора тестового данных проводились два вида атак:

- Атака по акустическому каналу – захват и анализ только акустических утечек, что позволяло оценить производительность исходного метода;
- Атака по акустическому и электромагнитному каналам – захват и анализ утечек обоих типов для оценки производительности модифицированного метода.

Измерения проводились путём фиксации времени начала и окончания главного цикла атаки с использованием инструментов C++ (библиотека time.h). Полученные данные были проанализированы с использованием методов обработки результатов физического эксперимента [13].

3.2. Экспериментальные результаты

Результаты экспериментальной обработки представлены в таблице 1.

Таблица 1 – Обработанные результаты эксперимента

№ Пары ключей	Тип атаки	$\bar{t}, s$
1	Акустика	3255.2 ± 14.42
	Комбинированный	2532.2 ± 10.53
2	Акустика	3257.8 ± 7.27
	Комбинированный	2532.2 ± 9.63
3	Акустика	3260.2 ± 9.3
	Комбинированный	2534.4 ± 5.78
4	Акустика	3275.2 ± 5.27
	Комбинированный	2542.2 ± 6.22
5	Акустика	3261.8 ± 5.7
	Комбинированный	2534.4 ± 7.01

Из таблицы видно, что среднее время, необходимое для проведения атаки с использованием комбинации акустического и электромагнитного каналов, меньше, чем при использовании исходного метода.

Для оценки изменения времени были рассчитаны абсолютные и относительные показатели:

$$t_{abs} = \overline{t_{ac}} - \overline{t_{comb}} \quad (13)$$

$$\delta = \frac{t_{abs}}{\overline{t_{ac}}} \quad (14)$$

где $\overline{t_{ac}}$ – время атаки только по акустическому каналу;

$\overline{t_{comb}}$ – время, затраченное на атаку по акустическому и электромагнитному каналам.

Погрешности оценок также рассчитывались методом переноса погрешностей [13]. В таблице 2 приведены абсолютные и относительные оценки ускорения с учётом погрешностей.

Таблица 2 – Оценки ускорения

№ Пары ключей	Тип оценки	Значение
1	Абсолютный $(t_{abs}), s$	723 ± 17.86
	Относительный (δ)	0.22 ± 0.06
2	Абсолютный $(t_{abs}), s$	725.6 ± 12.07
	Относительный (δ)	0.22 ± 0.004
3	Абсолютный $(t_{abs}), s$	725.8 ± 10.95
	Относительный (δ)	0.22 ± 0.003
4	Абсолютный $(t_{abs}), s$	733 ± 8.15
	Относительный (δ)	0.22 ± 0.003
5	Абсолютный $(t_{abs}), s$	727.4 ± 9.03
	Относительный (δ)	0.22 ± 0.003

Эксперимент подтвердил, что комбинированное использование акустического и электромагнитного каналов ускоряет атаку на RSA в GnuPG. Статистически значимое сокращение среднего времени выполнения атаки и уменьшение разброса результатов свидетельствуют об эффективности предложенного алгоритма.

Заключение

В ходе исследования был разработан и экспериментально проверен метод комбинирования акустического и электромагнитного анализа побочных каналов для ускорения атак на RSA-4096 в GnuPG.

Для реализации эксперимента был разработан программно-аппаратный стенд, включающий специализированное оборудование для синхронного захвата акустических и электромагнитных сигналов, а также программный комплекс на основе библиотек FFTW3 и libconfig.

Экспериментальная часть исследования показала, что совместное использование двух каналов утечки позволяет сократить среднее время атаки на 22% по сравнению с использованием только акустического канала. Данный результат был статистически подтверждён на выборке из 50 измерений, охватывающих пять пар ключей RSA-4096. Ускорение было достигнуто за счёт коррекции акустических сигналов с использованием

данных электромагнитного канала, что позволило сократить количество итераций перехвата и повысить точность идентификации битов секретного ключа.

Ограничения исследования связаны с использованием небольшого набора аппаратных платформ, ограниченного оборудования для определения электромагнитных утечек и лабораторных условий, что требует дальнейшей проверки метода в условиях, приближенных к реальным. Перспективным направлением представляется изучение влияния комбинирования других физических каналов на устойчивость криптоалгоритмов.

Результаты работы способствуют развитию методов анализа уязвимостей и могут быть использованы при проектировании защищённых криптографических реализаций, что особенно актуально в условиях роста угроз безопасности данных. В дальнейшем планируется расширить исследование на комбинирование с другими побочными каналами, например, с использованием информации из кеша процессора. Этот канал применялся в контексте уязвимости, связанной с оптимизацией RSA-CRT в GnuPG, исследованной в работе [14], а также был предложен метод обнаружения подобных атак «PREDATOR» [15], представляющий интерес для изучения возможностей его применения в рамках комбинирования каналов.

Благодарности

Работа выполнена в рамках государственного задания Министерства науки и высшего образования Российской Федерации № 075-00003-24-02 (проект FSEE-2024-0003).

Список литературы

1. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems / Kocher, Paul // Advances in Cryptology – CRYPTO’96 : 1996, Vol. 1109, P.104-113;
2. Optical fault induction attacks / S. Skorobogatov, R. Anderson // CHES: UK, 2003. p. 2-12;
3. Physical model of sensitive data leakage from PC-based cryptographic systems / Levina A., Sleptsova D., Mostovoy R., Tsvetkov L. // Journal of Cryptographic Engineering - 2019, Vol. 9, No. 4, pp. 393-400;
4. Remote timing attacks are practical / David Brumley and Dan Boneh // Proceedings of the 12th conference on USENIX Security Symposium : 2003, Vol. 12;
5. Remote timing attacks are still practical / Billy Bob Brumley and Nicola Tuveri // In ESORICS, pages 355–371, 2011;
6. A case study exploring side-channel attacks on pet wearables / Levina, A., Varyukhin, V., Kaplun, D., Zamansky, A., van der Linden, D. // IAENG International Journal of Computer Science, 2021, 48(4);
7. RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis / Genkin, D., Shamir, A., Tromer, E. // In: Garay, J.A., Gennaro, R. (eds) Advances in Cryptology – CRYPTO 2014. CRYPTO 2014. Lecture Notes in Computer Science, vol 8616. Springer, Berlin, Heidelberg;
8. Acceleration of the acoustic channel attack on the RSA algorithm in GnuPG software by combination with electromagnetic leaks / Krasov K.S., Levina A.B. // 8th International Conference on Communication and Network Technology, 2024;

9. Fundamentals of theoretical electrical engineering: A textbook. 2nd ed. / Yu.A. Bychkov, V.M. Zolotnitsky, E.P. Chernyshev, A.N. Belyanin // St.Petersburg: Lan Publishing House, 2008. 592 pages;
10. RFC 4880: OpenPGP Message Format / Callas, L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer // Nov. 2007. [Online]. URL: https://www.rfceditor.org/rfc/rfc4880.txt;
11. Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities / Coppersmith, D. // J. Cryptology 10, 233–260 (1997);
12. Accurate method for calculating the required number of repeated experiments / Boyko A. F., Kudennikov E. Yu. // Vestnik BSTU named after V. G. Shukhov;
13. Methods of processing the results of a physical experiment / Morozov V.V., Sheinman I.L., Sheinman J.S. // SPbSETU «LETI» named after V.I.Ulyanov (Lenin), Saint-Petersburg, Russia, 2020;
14. Cache Side-Channel Attack on Mail User Agent / H. Kim, H. Yoon, Y. Shin and J. Hur // 2020 International Conference on Information Networking (ICOIN), Barcelona, Spain, 2020, pp. 236-238;
15. PREDATOR: A Cache Side-Channel Attack Detector Based on Precise Event Monitoring / M. Wu, S. McCamant, P. -C. Yew and A. Zhai // 2022 IEEE International Symposium on Secure and Private Execution Environment Design (SEED), Storrs, CT, USA, 2022, pp. 25-36.